Lesley E. Weaver (SBN 191305)
BLEICHMAR FONTI & AULD LLP
555 12th Street, Suite 1600
Oakland, CA 94607
Tel.: (415) 445-4003
Fax: (415) 445-4020
lweaver@bfalaw.com

Derek W. Loeser (admitted *pro hac vice*)
KELLER ROHRBACK L.L.P.
1201 Third Avenue, Suite 3200
Seattle, WA 98101
Tel.: (206) 623-1900
Fax: (206) 623-3384
dloeser@kellerrohrback.com

Plaintiffs' Co-Lead Counsel

Additional counsel listed on signature page

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

IN RE: FACEBOOK, INC. CONSUMER PRIVACY USER PROFILE LITIGATION	MDL No. 2843 Case No. 18-md-02843-VC
This document relates to: ALL ACTIONS	**PLAINTIFFS' OPPOSITION TO MOTION OF DEFENDANT FACEBOOK, INC. TO DISMISS PLAINTIFFS' FIRST AMENDED CONSOLIDATED COMPLAINT** Judge: Hon. Vince Chhabria Courtroom: 4, 17th Floor Hearing Date: May 29, 2019 Hearing Time: 10:30 a.m.

Table of Contents

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

I. INTRODUCTION

Plaintiffs' First Amended Consolidated Complaint (ECF No. 257) ("FAC") describes in detail the concrete, particularized harms Facebook, Inc. ("Facebook") caused when it sold access to tens of thousands of data points derived from private content that Plaintiffs shared in non-public forums. Facebook promised Plaintiffs their Privacy Settings[1] controlled who could see what they shared, inducing Plaintiffs to share videos, photos, and other highly personal content. In fact, undisclosed to Plaintiffs, Facebook collected and aggregated this private content with other information to allow Facebook's Business Partners, App developers, and other unauthorized third parties to review, read, share, analyze, and psychographically target Plaintiffs. Facebook also enabled thousands of third parties, including highly disreputable ones like This is Your Digital Life, to permanently retain or sell users' private content, devoid of any monitoring and without a way to retrieve or destroy it. Facebook's conduct was not merely negligent, although it was certainly at least that. It created platforms that *deliberately* stripped Plaintiffs' Privacy Settings from photos, videos, and other content, enabling App developers and third parties to mine, analyze, and target users based on private content.

By irrevocably sharing content intended to be private and enabling its deanonymization, Facebook invaded Plaintiffs' legally protected privacy rights—while reaping billions of dollars in revenue from the invasion. Facebook also harmed Plaintiffs economically by taking Plaintiffs' property without their consent and in violation of their agreement. Plaintiffs would have engaged far less often and less intimately on Facebook's platform had Facebook told them that *no* communications are truly private. Because Facebook did not disclose its conduct, Plaintiffs could not have consented to Facebook's practices.

Rather than fully addressing Plaintiffs' allegations, Facebook's Motion to Dismiss (ECF No. 261) ("Motion" or "MTD") ignores those it finds inconvenient. Facebook tries to rewrite the FAC, claiming the same standards apply here as would apply to a simple data breach. That is not

[1] Capitalized terms, unless otherwise defined herein, have the same definition as ascribed to them in the FAC.

this case. Facebook fails to show that it secured users' express or implied consent, does not rebut Plaintiffs' injuries in fact, and fails to meet the legal standard for dismissal of Plaintiffs' claims. For the reasons set forth below, Facebook's Motion should be denied in its entirety.

II. STATEMENT OF FACTS

Facebook encouraged Plaintiffs to share their likes, interests, photos, videos, political beliefs, and other personal information with their Friends on Facebook by promising that users could control who could view this content using Privacy Settings. ¶¶ 282, 284.[2] In fact, Plaintiffs' Privacy Settings simply did not apply to how Facebook shared their content with Facebook's App developers and Business Partners. ¶¶ 31, 39, 47, 56, 64, 72, 81, 89, 97, 108, 116, 124, 132, 140, 148, 156, 164, 172, 180, 191, 198, 206, 215, 222, 230, 238, 249, 260.

For example, from 2010 to 2015, Facebook's developer platform allowed third parties to access the likes, comments, photos, video viewing history, and other sensitive content and information of the Friends of those who downloaded Apps.[3] Once an App accessed user content and information, nothing prevented App developers from downloading it and using it however they liked. Because Facebook stripped privacy metadata from photos and videos, third parties were not informed of privacy settings which should otherwise have restricted the use of that content. ¶ 428. These facts flatly contradict Facebook's repeated and false assertions that Plaintiffs' Privacy Settings were honored. These harms are ongoing.

Undisclosed to Plaintiffs, Facebook shared (and continues to share) Plaintiffs' content and information with Whitelisted Apps and Business Partners through private APIs.[4] ¶¶ 483, 496. Facebook did not inform Plaintiffs that it was sharing their private content with certain Whitelisted Apps or selected Business Partners after it had agreed, by consent decree with the Federal Trade Commission ("FTC"), to stop that practice. ¶¶ 31, 39, 47, 56, 64, 72, 81, 89, 97,

[2] Cites to "¶" refer to the FAC, ECF No. 257.

[3] Facebook's developer platform, called "Graph API," was the mechanism by which App developers could access user content and information. Facebook engineers designed and created this platform and were in sole control of how it functioned. ¶ 393.

[4] An application programming interface, or API, is a collection of commands that an application can run on Facebook to interface with Facebook and its users. ¶ 366 n.90.

108, 116, 124, 132, 140, 148, 156, 164, 172, 180, 191, 198, 206, 215, 222, 230, 238, 249, 260. Whitelisted Apps and Business Partners accessed Plaintiffs' information regardless of their Privacy Controls or App Settings—contrary to Facebook's assurances that users owned and could control their content and information using tools Facebook provided.[5] ¶¶ 343-44, 375, 377-78, 593; *see also* ¶¶ 496, 515-17, 554, 599, 600-02, 680. This is yet another example of Facebook violating Plaintiffs' Privacy Settings.

Facebook has still not identified all of the Whitelisted Apps. Nor did Facebook disclose how it enabled its Business Partners to use this information or monitor them. ¶¶ 322, 550, 562. In fact, Facebook only disclosed some of these partnerships, including those with Alibaba, Warner Bros., Yahoo!, and Yandex, after a Congressional inquiry. ¶ 484. Facebook worked hard to keep these partnerships and their terms concealed from Plaintiffs, including in this litigation.[6]

Facebook compounded the harm to Plaintiffs by giving their private content to unvetted App developers. Facebook failed to monitor Apps' use of that personal information once they obtained it.[7] ¶¶ 518, 537-40, 549, 554-55, 675. In this way, unscrupulous Apps could collect private photos, stripped of privacy metadata by Facebook, and post them in an App that allowed

[5] Facebook's argument that Plaintiffs admitted otherwise fails. Plaintiffs have consistently alleged that Facebook stripped privacy metadata and allowed Apps to disregard Privacy Settings. There are no admissions. Even if prior allegations were somehow inconsistent, factual assertions in pleadings may be "subsequently recharacterize[d]" by amendment. *Sicor Ltd. v. Cetus*, 51 F.3d 848, 859-60 (9th Cir. 1995); *cf.* MTD 34 n.18. (concerning inapplicable estoppel cases).

[6] Facebook has refused to produce these agreements and failed to produce meaningful discovery in this action. *See* Declaration of Lesley E. Weaver in Support of Plaintiffs' Opposition to Motion of Defendant Facebook, Inc. to Dismiss Plaintiffs' First Amended Complaint ("Weaver Declaration"). However, since filing the FAC, multiple regulatory investigations have been launched around the world, most recently a criminal investigation of Facebook's data deals with Business Partners. Michael LaForgia, Matthew Rosenberg and Gabriel J.X. Dance, *Facebook's Data Deals Are Under Criminal Investigation*, N.Y. Times (Mar. 13, 2019), https://www.nytimes.com/ 2019/03/13/ technology/facebook-data-deals-investigation.html. Facebook actively resists making any of this public. *See, e.g.*, Defendant Facebook, Inc.'s Opposed Motion to Seal, *D.C. v. Facebook*, 2018 CA 008715 B (D.C. Super. Ct. Mar. 11, 2019).

[7] New facts continue to emerge of ongoing harm related to Facebook's failure to monitor. *See, e.g.*, UpGuard, *Losing Face: Two More Cases of Third-Party Facebook App Data Exposure* (Apr. 3, 2019), https://www.upguard.com/breaches/facebook-user-data-leak.

users to scroll through and rate the photos without notice to Plaintiffs. ¶ 749.

Facebook's failure was willful. When former Facebook operations manager Sandy Parakilas raised concerns to executives at Facebook that user content was being exploited, Facebook felt it was "better not to know." ¶¶ 539-45. Since the Cambridge Analytica Scandal came to light, CEO Mark Zuckerberg acknowledged that if Facebook had implemented changes to its platform a year sooner, it "could have prevented the [Cambridge Analytica] situation completely." ¶ 572. Even now, Facebook has not yet told its own users what it disclosed to these third parties.

Plaintiffs did not know that Facebook would allow them to be psychologically manipulated based on their private content and information. ¶¶ 29, 37, 45, 53, 61, 70, 79, 87, 95, 106, 114, 122, 130, 138, 146, 154, 170, 178, 189, 196, 204, 213, 220, 228, 236, 247, 258. Psychographic marketing extends beyond typical targeted advertising based on demographics and allows third parties to target individual users based upon their individual fears, feelings, and values. ¶¶ 322, 324.

Facebook barters access to Plaintiffs' content in exchange for in-kind payment from third parties, including advertising expenditures, reciprocal data, and engineering labor that otherwise would have cost Facebook millions of dollars. ¶¶ 291, 486, 710. For example, Facebook grants Apps, including Whitelisted Apps, varying levels of access to users' content and information depending on the value they add to the platform and deliver to Facebook. ¶¶ 303, 502. Facebook also sells access to Plaintiffs' content and information to its Business Partners in exchange for like data. ¶ 487. By exploiting Plaintiffs' private content, Facebook drove its average revenue per user ("ARPU") higher. By 2018, Facebook's ARPU in the United States and Canada had grown from less than $5 in 2011 to $34. ¶ 332.

While Facebook has profited, Plaintiffs have been deprived of the benefit of their bargain and are irreparably harmed. This lawsuit seeks accountability, damages, protection, and restitution for users.

III. ARGUMENT

A. Plaintiffs Have Standing Under Article III.

A plaintiff may demonstrate standing under distinct theories for separate claims. *DaimlerChrysler v. Cuno*, 547 U.S. 332, 352 (2006) (standing is a claim-by-claim inquiry). An injury need not be economic in order to confer standing. *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 409, 414 n.5 (2013). Here, Plaintiffs have alleged three distinct injuries in fact: invasions of privacy, economic injury, and an increased risk of identity theft.

1. Plaintiffs Have Suffered Injury in Fact Due to the Invasion of Their Privacy.

Invasion of a privacy interest confers standing under Article III, even without further harm. *See Eichenberger v. ESPN*, 876 F.3d 979, 983 (9th Cir. 2017) ("*every* disclosure of an individual's 'personally identifiable information' and video-viewing history offends the interests that the statute protects"); *Van Patten v. Vertical Fitness Grp.*, 847 F.3d 1037, 1043 (9th Cir. 2017) (noting that "[a]ctions to remedy defendants' invasions of privacy, intrusion upon seclusion, and nuisance have long been heard by American courts," finding Article III standing); *In re Google Cookie Placement Consumer Privacy Litig.* ("*Google Cookie Placement*"), 806 F.3d 125, 134 (3d Cir. 2015) (noting that "the Supreme Court itself has permitted a plaintiff to bring suit for violations of federal privacy law absent any indication of pecuniary harm"); *Patel v. Facebook*, 290 F. Supp. 3d 948, 954 (N.D. Cal. 2018) (invasion of a protected privacy interest confers standing without any "additional injury").

Facebook created an expectation of privacy by—among other things—informing users that they own their content and information and that their Privacy Settings would control who had access to it. ¶ 593 (quoting the SRR). Yet, without Plaintiffs' consent, Facebook disclosed sensitive content and information to Whitelisted Apps, Business Partners, and other Apps—content and information that included "photographs with geolocation data and time stamps, videos users had uploaded, accessed, or liked, also with geolocation data and time stamps, Plaintiffs' religious and political beliefs, their relationships, posts, and the pages they had liked." ¶ 748. Facebook also allowed Apps to view millions of users' private communications on

Facebook Messenger. ¶¶ 513, 516. Indeed, Facebook actively frustrated Plaintiffs' privacy designations by stripping privacy metadata from user content and information. ¶ 429. *Google Cookie Placement* recognizes that use of privacy settings creates a reasonable expectation of privacy, and dissemination of personal information where a user expected privacy—exactly what happened here—confers Article III standing. *See* 806 F.3d at 150.[8]

Facebook offers several reasons that—despite the invasion of their privacy—Plaintiffs lack standing. First, Facebook argues that Plaintiffs consented to the disclosure of their content and information. MTD 8-10. As explained below, Plaintiffs did not consent, and Facebook errs by conflating the standing inquiry with distinct and fact-intensive merits questions.

Next, Facebook argues that Plaintiffs lack standing because disclosure of personal information alone cannot confer standing without consequential harm. MTD 10-12. Courts have rejected this argument. *See, e.g.*, *Eichenberger*, 876 F.3d at 983; *Patel*, 290 F. Supp. 3d at 953-54. Disclosure of private information is itself the injury. In arguing otherwise, Facebook asks this Court to ignore not only the controlling case law but also the will of Congress and the California Legislature, both of which have created statutes that recognize the intrinsically harmful nature of invasion of privacy. *See Van Patten*, 847 F.3d at 1042-43 ("[A] violation of the TCPA is a concrete, *de facto* injury" and a "plaintiff alleging a violation under the TCPA 'need not allege any *additional* harm beyond the one Congress has identified.'") (citation omitted). And none of these cases address the scope and personal nature of the information at issue in this case.

[8] Facebook's other standing authorities concerning the wrongful disclosure of *non*-personally identifiable information are inapposite. *Goodman v. HTC Am.*, 2012 WL 2412070, at *7 (W.D. Wash. June 26, 2012) (rejecting standing based on misappropriation of location data); *Low v. LinkedIn*, 2011 WL 5509848, at *4 (N.D. Cal. Nov. 11, 2011) (browser history not "linked to his identity by LinkedIn" by disclosure of "anonymous LinkedIn user ID"); *Spokeo v. Robins*, 136 S. Ct. 1540, 1550 (2016) (zip codes); *Hancock v. Urban Outfitters*, 830 F.3d 511, 512-13 (D.C. Cir. 2016) (same). The extent of the biographical information disclosed distinguishes Plaintiffs' allegations from Facebook's other cases. *See Antman v. Uber Techs*, 2015 WL 6123054, at *11 (N.D. Cal. Oct. 19, 2015) (names and driver's license numbers); *Dugas v. Starwood Hotels & Resorts Worldwide*, 2016 WL 6523428, at *5-6 (S.D. Cal. Nov. 3, 2016) (finding standing based on theft of name and credit card information); *cf. Frank v. Gaos*, 139 S. Ct. 1041, 1044 (2019) (concerning "Google's transmission of users' search terms in referrer headers" but not information sufficient to identify plaintiffs).

Facebook further argues that if invasion of privacy confers standing, every data-breach plaintiff will "automatically have standing." MTD 10. Facebook is mistaken. Not every data breach discloses information sufficiently sensitive to constitute an invasion of a legally protected privacy interest. *Cf.* ¶¶ 320, 325 (the content and information disclosed here contained an "unprecedented amount of personal content and information" about Plaintiffs' personal lives). And Facebook's actions are intentional acts of disclosure not common in data breach cases.[9]

Facebook, however, conflates standing with the merits of a privacy claim and argues that, because Plaintiffs' privacy claims fail on their merits, Plaintiffs lack standing. MTD 12-18. Facebook cites nothing to support the contention that Plaintiffs must prove every element of every claim, on the pleadings, to demonstrate standing. Moreover, as discussed below, Plaintiffs plausibly plead the required elements of these claims.

Finally, Facebook argues that Plaintiffs do not have standing to assert claims "as to any apps or device manufacturers" other than the This Is Your Digital Life App, because Plaintiffs do not allege that they used any of these Apps or devices. MTD 7. This is wrong. Every Plaintiff accessed Facebook through their mobile phones, and Apple, Samsung, AT&T, Sprint, T-Mobile, and Verizon are all Business Partners. ¶ 484, 563. *See Bates v. United Parcel Serv.*, 511 F.3d 974, 985 (9th Cir. 2007) ("In a class action, standing is satisfied if at least one named plaintiff meets the requirements."). And this misunderstands Plaintiffs' claims arising from Friend access, in that the Apps and Business Partners at issue were *used by Plaintiffs' Friends*, not by Plaintiffs themselves. Plaintiffs do not know what Apps and devices are used by their Friends, and

[9] Plaintiffs allege personal information was *actually* disclosed to third-party Apps and Business Partners, distinguishing this case from Facebook's authorities. *See Beck v. McDonald*, 848 F.3d 262, 274 (4th Cir. 2017) (after "extensive discovery," "no evidence that the information contained on the stolen laptop has been accessed or misused"); *Kamal v. J. Crew Grp.*, 918 F.3d 102, 116 (3d Cir. 2019) (plaintiff alleged "neither third-party access of his information, nor" complete credit card numbers); *In re Google Inc. Privacy Policy Litig.*, 2012 WL 6738343, at *1-2 (N.D. Cal. Dec. 28, 2012) (no allegations that personal information was deliberately disclosed to business partners); *Cohen v. Facebook*, 798 F. Supp. 2d 1090, 1097 (N.D. Cal. 2011) (disclosure to Facebook friends of use of Facebook's "Friend Finder"); *Rivera v. Google*, 2018 WL 6830332, at *5 (N.D. Ill. Dec. 29, 2018) ("face templates have not been shared with other Google Photos users or with anyone outside of Google itself").

Facebook has largely hidden what Apps and Business Partners obtained user content and information through Friends. In any event, more than one hundred Business Partners, thousands of Whitelisted Apps, and tens of thousands of other Apps accessed Facebook users' content and information through their Friends, making it virtually certain that Plaintiffs' content and information was disclosed to numerous Apps, Whitelisted Apps, and Business Partners. ¶¶ 343, 484, 497, 515, 601, 615. More detail is not required at this stage.

2. Plaintiffs Have Suffered Economic Injury for Purposes of Article III.

The existence of a market for personal information, combined with allegations that Facebook has diminished the value of Plaintiffs' personal information, establishes economic injury and confers Article III standing. *See In re Anthem Data Breach Litig.* ("*Anthem II*"), 2016 WL 3029783, *15 (N.D. Cal. May 27, 2016) (allegations of potential acts of fraud using plaintiffs' personally identifiable information ("PII") "could be read to infer that an economic market existed . . . and that the value of [p]laintiffs' PII decreased as a result of the . . . data breach"); *In re Google Android Consumer Privacy Litig.* ("*Google Android II*"), 2014 WL 988889, at *7 (N.D. Cal. Mar. 10, 2014) ("Although Plaintiffs do not allege facts that show they paid money directly to Google, the Court cannot conclude that Plaintiffs might not be able to show an ownership interest in at least some of Google's profits."); *Fraley v. Facebook*, 830 F. Supp. 2d 785, 798 (N.D. Cal. 2011) (standing is based on "economic value of an individual's commercial endorsement of a product or brand to his friends").

Plaintiffs meet this standard. They allege that a market for their content and information exists—a fact that should not be surprising, since the content and information has economic value. *See* ¶¶ 798-800. Facebook's CEO believed that it was worth at least $0.10 for each App to view a user's profile. ¶¶ 744, 909. Plaintiffs also allege that Facebook has diminished the value of Plaintiffs' content and information by making it available to third parties. Because exclusive access to the data confers a competitive advantage, the data has a "first seller advantage." ¶ 801. By distributing their data, Facebook has deprived Plaintiffs of that first seller advantage. *Id.* The amount of damages is a matter for expert analysis, not for resolution at the pleading stage.

Facebook relies on *In re Google Inc. Privacy Policy Litig.* ("*Google Privacy*"), 2015 WL 4317479, at *5 (N.D. Cal. July 15, 2015), to argue that "sharing" personal information cannot give rise to Article III standing. MTD 10. But *Google Privacy* concerned dispositively different information and dissemination. There, only names, email addresses, and physical locations were disclosed to Apps from which plaintiffs had made purchases. Here, Facebook disclosed far more extensive content and information to thousands of Whitelisted Apps and hundreds of Business Partners, allowing Facebook to monetize access to Plaintiffs' content and information. ¶¶ 343, 484, 497, 515, 601, 615.

3. Increased Risk of Identity Theft Establishes Article III Standing.

Plaintiffs also allege economic injury based on the market for their content and information more generally—because the scope of the content and information disclosed by Facebook is of the sort to make Plaintiffs more attractive targets for identity theft. Plaintiffs have suffered injury in fact because most of them have experienced fraudulent conduct associated with their Facebook account, and many have paid out of pocket to protect themselves. For standing, actual identity theft is not necessary. All that is needed is "a credible threat of real and immediate harm." *Krottner v. Starbucks*, 628 F.3d 1139, 1143 (9th Cir. 2010) (concerning "theft of a laptop containing [plaintiffs'] unencrypted personal data"); *Susan B. Anthony List v. Driehaus*, 573 U.S. 149, 158 (2014) (standing exists where "the threatened injury is 'certainly impending,' or there is a 'substantial risk' that the harm will occur") (citation omitted); *see also Walters v. Kimpton Hotel & Rest. Grp.*, 2017 WL 1398660, at *1 (N.D. Cal. Apr. 13, 2017) ("The Court respectfully disagrees that a plaintiff must actually suffer the misuse of his data or an unauthorized charge before he has an injury for standing purposes."); *Attias v. Carefirst*, 865 F.3d 620, 628 (D.C. Cir. 2017) (plaintiffs established standing where they alleged a substantial risk of identity fraud based solely on theft of health insurance subscriber ID numbers "even if their social security numbers were never exposed to the data thief").

The threat of actual harm is real, immediate, and ongoing. Plaintiffs have paid for credit monitoring and have spent time and money to protect themselves from the imminent threat of

identity theft and fraud. Twenty-six Plaintiffs "have already experienced additional security risks such as phishing attempts, increased phone solicitations, incidents of fraud or misuse, efforts by hackers trying to access or log in to their Facebook accounts, Friend requests from trolls or cloned or imposter accounts, and other interference with their Facebook accounts." ¶ 788. Two other Plaintiffs "have been notified that their content and information is available on the dark web." *Id.* And twelve Plaintiffs have paid for some type of monitoring service. ¶ 791.

Facebook argues there is no injury in fact based on the risk of identity theft because there are no allegations that Facebook stored Social Security numbers.[10] MTD 6. Facebook's focus on Social Security numbers is an attempt to distract from the scope of content and information Facebook disclosed through its platforms, not just to Cambridge Analytica, but at least tens of thousands of Apps and other third parties. Facebook allowed access to "identifying information such as names of pets, grandparents, mother's maiden name, etc. [which] greatly heightens the risk of identity theft and fraud to Plaintiffs because such information is often used as 'challenge questions' by financial and other institutions seeking to confirm identities." ¶ 784. And Facebook enabled the deanonymization of Plaintiffs' content and information so that it could be pooled with other data sources and linked to users' accounts. ¶¶ 784, 792. Facebook's focus on Social Security numbers ignores the additive nature of personal data; individuals are at a great risk of identity theft and other forms of malicious attacks where third parties benefit from sources such as Facebook data. ¶ 784.

B. Plaintiffs Did Not Expressly Consent to Facebook's Disclosure of Personal Information.

Because consent is an affirmative defense, Facebook bears the burden of establishing it. *See Hill v. NCAA*, 7 Cal. 4th 1, 40 (1994) (describing "consent" as a "defense[]" that a defendant may "plead and prove"); *Matera v. Google*, 2016 WL 5339806, at *17 (N.D. Cal. Sept. 23, 2016)

[10] Facebook questions the link between the Cambridge Analytica Scandal and the fraudulent activity that Plaintiffs experienced (MTD 7 n.2), but Facebook ignores the consistent experiences of the twenty-six Plaintiffs who have reported fraudulent activity on their Facebook accounts. The consistency in Plaintiffs' experiences easily pleads a plausible link.

(under Wiretap Act, defendant bears burden on consent).[11] Facebook has failed to establish express or implied consent as a matter of law.

In support of express consent, Facebook argues that both the SRR and Data Policy were binding contracts. Even if they were, however, users could not contractually agree to—and thus could not expressly consent to—misconduct that the SRR and Data Policy failed to disclose. *See Opperman v. Path, Inc.*, 205 F. Supp. 3d 1064, 1072-73 (N.D. Cal. 2016) (under privacy torts, consent is effective only if it was "to the particular conduct, or to substantially the same conduct," and "the alleged tortfeasor did not exceed the scope of that consent"); *Campbell v. Facebook*, 77 F. Supp. 3d 836, 848 (N.D. Cal. 2014) (agreements that did not disclose conduct could not provide express consent under Wiretap Act). And here, the SRR and Data Policy failed to disclose Facebook's misconduct.

1. Consent Goes to the Merits, Not to Standing.

Despite Facebook's contentions otherwise, its argument that Plaintiffs consented to its misconduct is relevant to the merits, not to the threshold question of standing. In deciding a plaintiff's standing, federal courts assume that a plaintiff will prevail on the merits. *See Warth v. Seldin*, 422 U.S. 490, 502 (1975); *accord, e.g.*, *Defenders of Wildlife v. Gutierrez*, 532 F.3d 913, 924 (D.C. Cir. 2008). In deciding Plaintiffs' standing here, therefore, this Court should assume that Facebook will not be able to establish its affirmative defense of consent. *Cf. Am. Farm Bureau Fed'n v. U.S. EPA*, 836 F.3d 963, 968 (8th Cir. 2016) (assuming for purposes of standing that the plaintiffs could establish their "asserted privacy interest under FOIA").[12]

[11] Under both the SCA and the Wiretap Act, consent is an affirmative defense because it is an exception to a general statutory prohibition. *Compare Matera*, 2016 WL 5339806, at *17 (consent is an exception under the Wiretap Act), *with* 18 U.S.C. § 2702(b)(3) (listing consent as an exception to the SCA's prohibition on divulgement). Plaintiffs rely on Wiretap Act case law under the assumption, shared by Facebook, that its substantive standard for consent is not materially different from the SCA's.

[12] *Leite v. Crane Co.*, 749 F.3d 1117 (9th Cir. 2014), MTD 8 n.4, does not concern standing and notes, "[t]he district court resolves a facial attack [on Rule 12(b)(1)] as it would a motion to dismiss under Rule 12(b)(6): Accepting the plaintiff's allegations as true and drawing all reasonable inferences in the plaintiff's favor." 794 F.3d at 1121.

2. Users Did Not Expressly Consent to Misconduct That the SRR and Data Policy Did Not Disclose.

The SRR and Data Policy failed to disclose what Facebook was really doing—either by representing that it would do the opposite of what it actually did or by simply remaining silent about certain conduct.

a. The SRR and Data Policy Failed to Disclose the Access That Facebook Gave to Apps and Websites.

1. Whitelisted Apps. The Data Policy represented that users could use their App Settings to prevent third-party Apps from accessing their data via a Friend that used the App. ¶ 599. But Facebook permitted Whitelisted Apps to access content and information even in violation of restrictions that users had placed on such sharing. ¶¶ 601-02; *see also* ¶¶ 494-517. Facebook makes no argument that Plaintiffs consented to its sharing with Whitelisted Apps.

2. Lack of privacy control. Neither the SRR nor the Data Policy disclosed that Privacy Controls could not control whether third-party Apps could access users' content and information. Facebook thus failed to inform users of what they needed to do to protect their privacy. Facebook argues that the SRR sufficiently explained the distinction between Privacy Controls and App Settings. MTD 28. It did not. The statement on which Facebook relies states only that Privacy Controls *and* App Settings could be used to "control how" content and information "is shared." *Id.* This statement is actively misleading. Its use of "and" could be read to suggest that *both* Privacy Controls and App Settings separately could control how users' content and information was shared. At best, the statement fails to inform Plaintiffs that Privacy Controls *alone* were insufficient to restrict access to users' content and information. To secure consent, Facebook was obliged to affirmatively disclose this fact—particularly since users, in accordance with the plain meaning of "privacy," would reasonably assume that settings related to "privacy" would "control" how content and information would be shared with the outside world (*i.e.*, to Apps and websites). *See Park Univ. Enters. v. Am. Cas. Co. of Reading*, 314 F. Supp. 2d 1094, 1110 (D. Kan. 2004) ("The plain and ordinary meaning of privacy includes the right to be left alone, unburdened by unsolicited facsimiles."). Facebook cannot establish the agreement to

particular conduct required for express consent. Instead, Facebook relies on the remarkable proposition that a statement that implies user control over personal data is actually the basis for users' consent to surrender that control to Facebook.

Facebook now claims Privacy Controls only govern "who sees users information on Facebook." MTD 28. Facebook for years told users *exactly the opposite* of what they now argue. Facebook stated that "applications" must act "in accordance with your privacy settings," ¶ 626, or that users could limit data-sharing with applications "through [their] privacy settings," ¶ 630. These disclosures defeat express consent for users that signed up for Facebook prior to April 2010 because when the SRR and Data Policy were later updated to add new disclosures, Facebook did not provide notice to users of these changes, beyond merely posting a revised Data Policy or SRR to Facebook. ¶ 623. For these users, those new disclosures constituted "a revised contract," which is "merely an offer and does not bind the parties until it is accepted." *Douglas v. Dist. Court*, 495 F.3d 1062, 1066 (9th Cir. 2007) (citation omitted). Further, proper notice of a new contractual offer cannot be provided "by merely posting a revised contract on [a] website," as Facebook did here. *Id.* at 1065. Without proper notice of Facebook's offer, the users did not accept the new terms. This is true even if the SRR or Data Policy had purported to allow Facebook to modify those documents merely by posting a new version. *Roling v. E*Trade Sec.*, 756 F. Supp. 2d 1179, 1191 (N.D. Cal. 2010) (finding a contractual provision that allows a party to unilaterally change the terms of the contract without notice is not enforceable).[13]

3. Metadata stripping. The SRR represented that applications would "respect" users' privacy, and that users' agreement with Apps would control how the Apps could use, store, and transfer content and information. ¶ 612. In fact, because Facebook "stripped" privacy metadata

[13] Facebook cites *In re Facebook Biometric Info. Privacy Litig.*, 185 F. Supp. 3d 1155 (N.D. Cal. 2016), MTD 26, which found, after an evidentiary hearing, that Facebook sent users *individual* notice of one particular contractual revision in January 2015, beyond merely updating the policies. *Facebook Biometric Info.*, 185 F. Supp. 3d at 1167. Even if this finding bound this Court, which it does not, it would say nothing about *other* changes to the Data Policy and SRR *before* January 2015. Facebook made these changes without providing individual notice of any kind. ¶ 623. That factual allegation must be taken as true at this stage.

from photos and videos, ¶¶ 607-10, Apps could not respect users' privacy and abide by their Privacy Settings—after all, they could not know what users' Privacy Settings were. ¶ 611.

Facebook does not deny that it stripped users' privacy metadata from photos and videos and offers the astonishing retort that its representation merely means that Apps had to abide by Facebook's platform policy, not users' Privacy Settings. MTD 21. Even if that were a plausible reading of the statement, Facebook still did not affirmatively disclose that users' privacy metadata would be stripped. Facebook says it also told users that an App's user agreement controlled how their data would be used. This assertion fails for two reasons. First, it fails to show that *Friends* of App users—who did not have agreements with the Apps—were told that their privacy metadata would be stripped. *See* ¶¶ 621-22. Second, Plaintiffs allege that many Apps did not affirmatively tell users that their Privacy Settings would be ignored—so these Apps' agreements with their users failed to secure consent to metadata stripping. ¶ 612.

4. No consent to broad use. The Data Policy represented that if a user's Friend allowed a third-party App or website to access the user's content and information, the App or website was allowed to use that content and information only "in connection with" the Friend that granted permission. ¶¶ 596-97. Plaintiffs did not consent to broader use of that information. Thus, they did not consent to Facebook's allowing GSR and Cambridge Analytica to use their data in a manner far more broadly than just "in connection with" the Friend that had used the This Is Your Digital Life App. ¶ 598.

Facebook's unsatisfying explanation is that its representation was about what Apps and websites were *allowed* to do, not what they were *able* to do. MTD 21. Quite right. The Data Policy did not disclose the conduct in which GSR and Cambridge Analytica actually engaged, aided by Facebook's willful inaction. That is why Plaintiffs could not consent to that conduct.

5. Apps and websites that were advertisers. The SRR and Data Policy represented that Facebook would not give users' personally identifiable content and information to advertisers without users' consent. ¶¶ 603-04. Facebook violated this representation. It *did* allow advertisers to access users' personally identifiable content and information, so long as the advertisers were

Business Partners or third-party Apps or websites. ¶¶ 605-06. It failed to disclose that its representation contained this enormous loophole. *Id.*

Facebook counters that it sufficiently disclosed this loophole because it informed users that it shared their information with third-party Apps and websites. MTD 22. This mischaracterizes the disclosure and dodges the issue. Facebook's disclosure does not state that Apps and websites that advertised on Facebook could access Plaintiffs' private content *despite* the separate pledge that advertisers would not receive their content. *See In re Google Inc. Gmail Litig.* ("*Google I*"), 2013 WL 5423918, at *14 (N.D. Cal. Sept. 26, 2013) (a statement that "could mislead users" did not secure consent).

6. Psychographic profiling. The SRR and Data Policy did not disclose the extraordinarily intrusive uses of Plaintiffs' content and information that Facebook sold to third-party Apps and websites. Specifically, Facebook failed to disclose that it enabled those entities to use private content to engage in psychographic profiling and targeting of users. ¶ 619; *see also* ¶¶ 751-77.

Facebook does not deny the alleged conduct. It responds that it told users that it provided information to advertisers, and it helps advertisers target users benignly. MTD 22. But as Facebook admits, it told users that when it provided information to advertisers and helped them target users, it would not disclose users' PII. *Id.* In fact, Facebook enabled Apps and Business Partners to aggregate Plaintiffs' private content with other information, using it to psychographically profile and target them, through Facebook's tools. *See* ¶¶ 752-59, 770. These practices effectively deanonymize users. Facebook did not disclose this conduct, and so did not secure users' consent to it. *Cohen*, 798 F. Supp. 2d at 1095-96 (disclosure that names and profile pictures would be shared did not disclose that Facebook would use them as it did).

b. The SRR and Data Policy Failed to Disclose the Access that Facebook Gave to Business Partners.

1. Failure to disclose. Facebook never disclosed that it shared Plaintiffs' private content with Business Partners. Before 2015, Facebook represented that it might give users' information to "the people and companies that help us provide, understand and improve the services we offer," including "outside vendors" who "help host our website, serve photos and videos, process

payments, analyze data, conduct and publish research, measure the effectiveness of ads, or provide search results." ¶ 616 (quoting the pre-2015 Data Policy). Beginning on January 30, 2015, Facebook changed this language slightly to say that it might send users' content and information to "[v]endors, service providers, and other partners who globally support our business." *Id.* (quoting the post-January 30, 2015 Data Policy). But these Business Partners are not merely vendors.

Facebook claims that these disclosures were sufficient to inform reasonable users that access to their private information would be sold to Business Partners. Facebook is incorrect. For one thing, this language is simply "not specific enough," *Campbell*, 77 F. Supp. 3d at 847, to create consent to Facebook's sharing private content with a wide range of companies, including entertainment companies, software makers, chip designers, and digital-commerce entities. ¶ 617. Further, Business Partners received far more data than what was necessary to "globally support" Facebook's business. ¶ 616; *see also* ¶ 556 (Business Partners received "information beyond what was necessary for the specific purpose for which Facebook has asserted access was granted"). Thus, even if Facebook had properly disclosed the range of Business Partners, these entities' access still exceeded Plaintiffs' express consent. *See, e.g.*, *Backhaut v. Apple, Inc.*, 74 F. Supp. 3d 1033, 1046 (N.D. Cal. 2014) (when document disclosed that Apple would intercept messages for a particular reason, users did not agree to interception for *other* reasons).[14]

Even if one assumes *arguendo* that the Data Policy properly disclosed sharing with Business Partners at some point in the Class Period, users who signed up before September 7, 2011 never consented, because they were not notified of later revisions to the Policy. ¶¶ 634-38; *see supra* Section III.B.2.a (explaining why notice of contractual revisions is needed for express consent).

2. Lack of privacy control. Even if Facebook had properly disclosed its Business Partner sharing, Plaintiffs would not have been able to prevent Facebook from sharing their content and information. Despite representations in the SRR and Data Policy that users controlled access to

[14] The same is true for implied consent. *Google I*, 2013 WL 5423918, at *13.

their content, ¶¶ 593-94, no controls existed that prevented Business Partner sharing. ¶¶ 343-44, 595. Facebook offers no response to Plaintiffs' consent-related allegations on this point.

3. Business Partners that were advertisers. Facebook represented that it did not allow advertisers to access users' content. As noted above, however, it allowed advertisers precisely this kind of access if the advertisers were also Business Partners. ¶¶ 605-06. Facebook suggests that users consented to this access because it disclosed its Business Partner sharing but it did *not*, for reasons already given. And even if it had, similar to its purported disclosure as to Whitelisted Apps, Facebook ignores the core problem with its "disclosure": it failed to disclose that Business Partners that advertised on Facebook could access Plaintiffs' private content *despite* the separate pledge that advertisers could not access such content.

3. Because the Data Policy Was Not Part of a Contract and Was Not Reasonably Prominent or Accessible, Plaintiffs Did Not Expressly Consent to Behavior That the Data Policy, but Not the SRR, Disclosed.

To establish consent, Facebook relies on certain statements that appeared in the Data Policy but not in the SRR. These statements did not provide express consent because the Data Policy was not part of a binding contract. As Plaintiffs explained in their earlier opposition, users did not contractually assent to the Data Policy when they signed up. *See* ECF No. 208 at 10-12. Nor did users assent to the Data Policy by assenting to the SRR, because the SRR did not incorporate the Data Policy by reference. *Id.* at 12-14.

C. Facebook Fails to Show That Plaintiffs Impliedly Consented to Disclosure of Their Personal Information.

1. The SRR and Data Policy Did Not Create Implied Consent.

Implied consent requires that the SRR and Data Policy put users on "adequate notice" of Facebook's misconduct.[15] *See Campbell*, 77 F. Supp. 3d at 847 ("the 'critical question with respect to implied consent is whether the parties whose communications were intercepted had

[15] Implied consent is typically unripe for resolution at the pleading stage. *See In re Google Inc. Gmail Litig.* ("*Google II*"), 2014 WL 1102660, at *16 (N.D. Cal. Mar. 18, 2014) (describing implied consent as an "intensely factual question"); *see also Watkins v. L.M. Berry & Co.*, 704 F.2d 577, 582 (11th Cir. 1983) (reversing 12(b)(6) ruling in favor of implied consent and noting that "[i]t is the task of the trier of fact to determine the scope of the consent and to decide whether and to what extent the interception exceeded that consent").

adequate notice of the interception'") (quoting *Google I*, 2013 WL 5423918, at *12). Even if the SRR and Data Policy were sufficiently accessible and prominent to give adequate notice (and they were not), they still would not have created implied consent for fundamentally the same reason that they did not create express consent: they did not disclose, and thus failed to give fair notice of, Facebook's misconduct. *See* Section III.B.2, *supra*. Indeed, Facebook's own authorities demonstrate that documents cannot create notice of what they fail to disclose. *See Suzlon Energy v. Microsoft*, 671 F.3d 726, 731 (9th Cir. 2011) (no implied consent where "Microsoft never told Sridhar that his communications might be monitored or disclosed").

As noted above, moreover, certain disclosures were added to the SRR and Data Policy *after* large numbers of users initially signed up.[16] *See supra* Section III.B.2.b. Even assuming that these users were put on notice of the contents of these documents when they first signed up, they were not put on notice of *additions* made to those documents *after* signing up—and thus did not impliedly consent to whatever those additions newly disclosed. Implied consent was not created by the mere presence of the amended Data Policy and SRR on the website. The mere presence of certain documents on a website, even if those documents are hyperlinked on every page of the website, cannot provide constructive (let alone actual) notice of the content of those documents. This is the sensible conclusion reached by the *Opperman* court: "[W]here a website makes its terms of use available via a conspicuous hyperlink on every page of the website but otherwise provides no notice to users nor prompts them to take any affirmative action to demonstrate assent," the hyperlink "is insufficient to give rise to constructive notice." *Opperman*, 205 F. Supp. 3d at 1074 (quoting *Nguyen v. Barnes & Noble*, 763 F.3d 1171, 1178-79 (9th Cir. 2014)). The mere posting of revised Data Policies and SRRs, without more, did not create implied consent, and bears no resemblance to the repeated clear warnings that courts have held sufficient to create such consent.[17] And, Facebook does not explain, for each change, how

[16] Plaintiffs preserve all objections to the exhibits attached to the declaration of Michael Duffey, made in their opposition to Facebook's pending Request for Judicial Notice in Support of Its Motion to Dismiss. *See* ECF Nos. 185-187, 210, 235, 236.

[17] *United States v. Van Poyck*, 77 F.3d 285, 292 (9th Cir. 1996) (finding implied consent when a prison posted warning signs directly above phones prisoners were using "warning of the

retroactive consent was obtained—such as when the change was posted and whether it was material.

2. The App Settings Did Not Create Implied Consent.

Facebook argues that the App Settings independently created implied consent. Even under Facebook's theory, the App Settings at most notified users of the bare fact that third-party Apps could access their own content.[18] They did *not* inform Plaintiffs that their Privacy Controls alone were insufficient to restrict Apps' access to private content. Facebook cites the App Settings' instructions, which note that the App Settings could control the access that Apps could have to users' content and information. MTD 28-29. That statement, however, does not say that changing App Settings was necessary even if a user had already selected non-public settings on her Privacy Controls. ¶ 640. Facebook speculates that "[a]ny Plaintiff who modified his or her Timeline settings . . . would have seen that the 'Privacy' tab did not contain all privacy controls." MTD 30. But even if users had been aware of the existence of something called "App Settings," the webpages that Facebook cites do not disclose that these settings had anything to do with restricting access to users' content and information. In any event, what a reasonable user might have inferred from these conflicting disclosures is a question of fact.

3. Because the Data Policy Was Not Reasonably Noticeable or Accessible, It Did Not Create Implied Consent.

Facebook argues that even if the Data Policy was not a contract and could not create express consent, *see supra* Section III.B.2, users were on notice of—and thus gave their implied consent to—its terms. But the Data Policy was not prominently displayed. The hyperlink to the

---

monitoring and taping"); *Nei Contracting & Eng'g v. Hanson Aggregates Pac. Sw.*, 2016 WL 4886933, at *3 (S.D. Cal. Sept. 15, 2016) (holding after a bench trial that plaintiffs failed to show lack of consent and noting "[i]n the typical implied in fact consent scenario, a party is informed that his call will be recorded, and he continues to use the communication system after receiving notice the communications are being intercepted").

[18] Thus, the App Settings could not have notified users that Apps were using their data more broadly than "in connection with" the Friends who download the Apps, that Apps were also advertisers, that Facebook stripped privacy metadata, or that Apps were engaging in psychographic profiling—let alone disclosed the special access that Facebook had granted to Whitelisted Apps or Business Partners.

Data Policy on Facebook's home screen was in small print on the bottom on the website. ¶ 658. Indeed, "[i]t would take a user at least eighteen separate clicks of the mouse to read the entire Data Policy." ¶ 662. Additionally, "from June 2012 to January 2015, a user would need to click back and forth at least twelve times in order to read the full contents of the Data Policy contained within six separate subheadings." ¶ 663. Facebook users would have had to stitch together the Data Policy's disclosures piecemeal. It is not surprising that most of the Plaintiffs were not on actual notice of the Data Policy's existence. ¶¶ 28, 36, 44, 61, 69, 78, 86, 94, 105, 113, 121, 137, 145, 153, 161, 169, 177, 188, 195, 203, 219, 227, 235, 246, 257.

At sign-up, users could have been on notice of the Data Policy only if they noticed the small-print reference to it (from March 2009 until February 2012) or had clicked on the hyperlink to it (from February 2012 to April 2018). But the 2009-2012 small-print reference was not reasonably conspicuous so as to put users on notice, *see supra* Section III.C.1, and the mere presence of a hyperlink from 2012 to 2018 cannot have created notice. *Opperman*, 205 F. Supp. 3d at 1073-74. After signing up, the Data Policy simply became a hyperlink at the bottom of Facebook's webpage, which was insufficient to create notice. *See id.*

4. The FTC Consent Decree Did Not Create Implied Consent.

Facebook maintains that a piece of information *outside* the SRR and Data Policy—the 2011 FTC Complaint—created implied consent to its conduct because it put users on notice "that Facebook employed two separate sets of controls . . . and that Facebook shared data with third-party apps even if users' Privacy Settings were set to 'Friends Only.'" MTD 31. While implausible, even if the 2011 FTC Complaint *did* put users on notice of these facts, it would not have created consent to Cambridge Analytica's broad use of user data, access by Apps that were also advertisers, access by Whitelisted Apps, metadata stripping, or psychographic profiling. *See supra* Section III.B.2. Nor would it have created consent to Facebook's Business Partner sharing.

Rather than creating implied consent, the 2011 FTC action did precisely the opposite. The FTC Consent Decree was publicized at the same time as the FTC Complaint. *See* MTD 31 n.14. Under the Decree, Facebook agreed *not* to share user data with third-party Apps and

websites unless Facebook had "clearly and prominently disclose[d] to the user, separate and apart from" the SRR and Data Policy, the information that Facebook would disclose and the third parties to which the information would be disclosed. ¶ 677. The 2011 FTC action, if anything, assured users that Facebook was *not* sharing their content with third-party Apps and websites.

D. Facebook Cannot Hide Behind an Exculpatory Clause.

Facebook maintains that an exculpatory clause in the SRR bars all Plaintiffs' claims, relying on a provision that "Facebook is not responsible for the actions . . . of third parties." *See* MTD 23, 37-38. But Plaintiffs seek redress because of *Facebook's* actions. Facebook gave third parties users' private content without disclosure or consent. Its attempt to shirk responsibility is untenable, as Facebook now must realize.[19] *In re Facebook PPC Advert. Litig.*, 2010 WL 3341062, at *5 (N.D. Cal. Aug. 25, 2010) (holding "disclaimer does not cover [Facebook's] own actions"); *Bailey v. United States*, 289 F. Supp. 2d 1197, 1212 (D. Haw. 2003) (distinguishing "situation in which a party seeks a waiver of liability for its own actions"). An exculpatory clause cannot bar claims for violations of statutory law or claims sounding in gross negligence or fraud. *See City of Santa Barbara v. Superior Court*, 41 Cal. 4th 747, 776-77 (2007).

Even if third parties' conduct were at issue, the SRR's exculpatory clause is invalid under *Tunkl v. Regents of University of Cal.*, which set out six public interest factors that invalidate exculpatory clauses. 60 Cal. 2d 92, 97-102 (1963) (noting contract at issue "need only fulfill some" of six characteristics to invalidate exculpatory clause). Facebook's SRR meets all of the *Tunkl* factors. Facebook performs a "service of great importance to the public" that for some, including 70 million small businesses, is a "practical necessity." *Id.* at 98-99. As Mark Zuckerberg acknowledges, Facebook is an essential forum for public discourse and commerce. *See* Testimony of Mark Zuckerberg before the H. Comm. on Energy & Commerce, 2018 WL 1740473 (Apr. 11, 2018); *see also* ¶¶ 1, 966(B). A service need not be a "necessity of life" for it

[19] *See* European Comm'n, *Facebook Changes Its Terms and Clarifies Its Use of Data for Consumers Following Discussions with the European Commission and Consumer Authorities* (Apr. 9, 2019), http://europa.eu/rapid/press-release_IP-19-2048_en.htm (announcing, *inter alia*, Facebook's amendment to limitation of liability, acknowledging "responsibility in case of negligence, for instance in case data has been mishandled by third parties").

to be a "practical necessity" under *Tunkl*. *See Pelletier v. Alameda Yacht Harbor*, 188 Cal. App. 3d 1551 (1986) (invalidating exculpatory clause related to yacht berth). Facebook likewise "possesses a decisive advantage of bargaining strength" against users due to the essential nature of the service. *Tunkl*, 60 Cal. 2d at 99-100. Users cannot go elsewhere for comparable services. The sheer number of Facebook users—2.2 billion—creates a network effect that no other social media platform has been able to replicate.

Facebook holds itself out as willing to provide services "for any member of the public who seeks it," *Tunkl* at 98-99, and its SRR is "a standardized adhesion contract." *id.* at 100. Facebook users' data is also placed "under the control" of Facebook and is "subject to the risk of carelessness" by Facebook. *Id.* at 101. Facebook users have no meaningful control over the content Facebook encourages them to generate on its site. *See* ¶¶ 342-83, 439, 494-517, 966(F). Finally, as Facebook acknowledges in its Motion and elsewhere,[20] Facebook's business is of a type generally "thought suitable for public regulation." MTD 38 (quoting *Tunkl*, 60 Cal. 2d at 98). Indeed, it is subject to FTC regulation and an intricate web of laws.[21] *See Gardner v. Downtown Porsche Audi*, 180 Cal. App. 3d 713, 717 (1986) (auto repair shop is business suitable for public regulation).

Facebook's contractual waiver is procedurally and substantively unconscionable. Procedurally, the provision is oppressive due to users' complete lack of bargaining power, and substantively, it is one-sided. *See, e.g.*, *A & M Produce v. FMC*, 135 Cal. App. 3d 473, 493 (1982) (finding disclaimer provision unconscionable where "nonnegotiable terms on preprinted form agreements combine with disparate bargaining power [and] result[] in the allocation of commercial risks in a socially or economically unreasonable manner"); *see also Lhotka v.*

[20] Mark Zuckerberg, *Mark Zuckerberg: The Internet needs new rules. Let's start in these four areas*, Wash. Post (Mar. 30, 2019), https://www.washingtonpost.com/opinions/mark-zuckerberg-the-internet-needs-new-rules-lets-start-in-these-four-areas/2019/03/29/9e6f0504-521a-11e9-a3f7-78b7525a8d5f_story.html (calling for regulation of Facebook).

[21] For example, Facebook is subject to the Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501-6506, the Illinois Biometric Information Privacy Act of 2008, 740 Ill. Comp. Stat. 14/1, and the recently enacted California Consumer Privacy Act of 2018, 2018 Cal. Legis. Serv., ch. 55.

Geographic Expeditions, 181 Cal. App. 4th 816, 826 (2010).

E. Facebook Violated Federal Statutes.

1. Plaintiffs Have Standing to Bring VPPA and SCA Claims.

Plaintiffs have Article III standing under the Video Privacy Protection Act ("VPPA"), 18 U.S.C. § 2710 (2012), and the Stored Communications Act ("SCA"), *id.* §§ 2701-11. Facebook only challenges the "injury in fact" element of standing. MTD 6-18; *Spokeo*, 136 S. Ct. at 1547. But because the VPPA and SCA codify a substantive right—a privacy right whose violation has long been recognized as a freestanding injury—Plaintiffs need not plead additional harm beyond a statute's violation to establish standing. *See Eichenberger*, 876 F.3d at 983.

Allegations that Facebook violated § 2710(b)(1) of the VPPA are sufficient to satisfy the injury in fact element of standing. "[E]very 18 U.S.C. § 2710(b)(1) violation 'present[s] the precise harm and infringe[s] the same privacy interests Congress sought to protect' by enacting the VPPA." *See Eichenberger*, 876 F.3d at 984; *see also* ¶ 861. Thus, "the VPPA identifies a *substantive* right to privacy that suffers *any time* a video service provider discloses otherwise private information." *Id.*[22] Under *Eichenberger*, consent is not part of the Article III analysis, because § 2710(b)(1) of the VPPA separately "codifies a context-specific extension of the *substantive* right to privacy." *Id.* at 983.[23] Facebook's argument that consent is part of the standing analysis is wrong. Even if it were not, Facebook has failed to meet its burden of proving consent, as detailed above in Section III.B. *See* 18 U.S.C. § 2710(b)(2)(B)(i); *Matera*, 2016 WL 5339806, at *17 ("[T]he party seeking the benefit of the exception" bears the burden of

[22] The two other circuits to have considered this issue have held the same. *Perry v. Cable News Network*, 854 F.3d 1336, 1341 (11th Cir. 2017); *In re Nickelodeon Consumer Privacy Litig.* ("*Nickelodeon II*"), 827 F.3d 262, 274 (3d Cir. 2016).

[23] *Cf. Stacy v. Dollar Tree Stores*, 274 F. Supp. 3d 1355, 1363 (S.D. Fla. 2017) ("FCRA's stand-alone document requirement does not automatically cause a concrete injury for purposes of Article III standing"); *Larroque v. First Advantage LNS Screening Sols.*, 2016 WL 4577257, at *5 (N.D. Cal. Sept. 2, 2016) (FCRA disclosure violation does not automatically create injury, requiring separate privacy analysis); *Nokchan v. Lyft*, 2016 WL 5815287, at *9 (N.D. Cal. Oct. 5, 2016) (same); *In re Michaels Stores, Fair Credit Reporting Act (FCRA) Litig.*, 2017 WL 354023, at *9-10 (D.N.J. Jan. 24, 2017) (same); *Jaras v. Equifax*, --- F. App'x ----, 2019 WL 1373198, at *2 (9th Cir. Mar. 25, 2019) (same).

demonstrating consent.) (citation omitted). Remarkably, Facebook does not contest that it failed to obtain express consent from users as required by the VPPA. MTD 18 n.8. Facebook instead asserts that is entitled to the VPPA's lawful consent exception, ignoring its "deficiency" in satisfying the requirements of § 2710(b)(2)(B)(i). *Id.*

In accordance with *Eichenberger*—and, as courts in the Ninth Circuit and the Northern District of California have repeatedly held—a defendant's violation of the substantive provisions of the SCA is sufficient to satisfy the injury in fact element of standing.[24] Like the VPPA, the SCA codifies an extension of the substantive right of privacy to electronic communications.[25] *Theofel v. Farey-Jones*, 359 F.3d 1066, 1072-73 (9th Cir. 2004) (analogizing to "the tort of trespass," the SCA "protects individuals' privacy and proprietary interests," and "reflects Congress's judgment that users have a legitimate interest in the confidentiality" of electronic communications). Here, Facebook violated Sections 2702(a)(1) and (a)(2) of the SCA "by knowingly divulging the contents, including content and information, of Plaintiffs' electronic communications . . . to unauthorized parties." ¶¶ 847-48. For the reasons articulated by the Ninth Circuit in *Theofel* and *Eichenberger*, the violation alleged here is of a substantive, rather than a procedural, right under the SCA.[26]

Facebook's claim that the SCA "does not exhibit congressional judgment about who may

---

[24] *See* 876 F.3d at 982-84; *see, e.g.*, *In re Facebook Internet Tracking Litig.*, 263 F. Supp. 3d 836, 842 (N.D. Cal. 2017); *In re Zynga Privacy Litig.*, 750 F.3d 1098, 1105 (9th Cir. 2014); *Jewel v. Nat'l Sec. Agency*, 673 F.3d 902, 908-09 (9th Cir. 2011); *Svenson v. Google*, 2015 WL 1503429, at *2 (N.D. Cal. Apr. 1, 2015); *Perkins v. LinkedIn*, 53 F. Supp. 3d 1190, 1207-08 (N.D. Cal. 2014); *In re Google Inc. Privacy Policy Litig.*, 2013 WL 6248499, at *8-9 (N.D. Cal. Dec. 3, 2013); *In re iPhone Application Litig.* ("*iPhone II*"), 844 F. Supp. 2d 1040, 1055 (N.D. Cal. 2012); *In re Facebook Privacy Litig.*, 791 F. Supp. 2d 705, 711-12 (N.D. Cal. 2011), *aff'd*, 572 F. App'x 494 (9th Cir. 2014).

[25] Notably, Facebook does not argue that the rights codified by 18 U.S.C. § 2701(a)(1) and § 2701(a)(2) are procedural, rather than substantive. MTD 15-18.

[26] *See Theofel*, 359 F.3d at 1072-73; *Eichenberger*, 876 F.3d at 983 ("Historical practice confirms" that "[v]iolations of the right to privacy have long been actionable at common law," and "the Supreme Court has noted that 'both the common law and the literal understanding of privacy encompass the individual's control of information concerning his or her person.'") (citations omitted); *see also Nickelodeon II*, 827 F.3d at 273-74 (alleged violation of SCA "sufficient to establish Article III standing").

bring suit" because of its "person aggrieved" language also fails. MTD 16-17. The Ninth Circuit has held that analogous language in § 2710(b)(1) of the VPPA reflects Congress's judgment that this is "a substantive provision that protects concrete interests." *See Eichenberger*, 876 F.3d at 983. Facebook does not dispute that Plaintiffs are "person[s] aggrieved" by its violations of the SCA, ¶ 837, nor does it dispute that Plaintiffs "fall[] within the 'zone of interests' sought to be protected" by the SCA. *See Thompson v. N. Am. Stainless*, 562 U.S. 170, 177 (2011) (citation omitted). Facebook's remaining arguments should not be credited, for the reasons discussed in Sections III.A and III.E.3.

2. Facebook Violated the Video Privacy Protection Act.

Facebook violated the VPPA, a statute designed to address "Congress's concern with protecting consumers' privacy in an evolving technological world." *In re Hulu Privacy Litig.*, 2012 WL 3282960, at *6 (N.D. Cal. Aug. 10, 2012).

a. Facebook Is a Video Tape Service Provider.

A "video tape service provider" under the VPPA is "any person, engaged in the business, in or affecting interstate or foreign commerce, of rental, sale, or *delivery* of prerecorded video cassette tapes or similar audio visual materials." 18 U.S.C. § 2710(a)(4) (emphasis added). The "video tape service provider" clause of the VPPA has been interpreted broadly to apply to companies such as Facebook that deliver video, including Hulu, Vizio, and Amazon. *See Hulu*, 2012 WL 3282960, at *6; *In re Vizio, Consumer Privacy Litig.*, 238 F. Supp. 3d 1204, 1221-22 (C.D. Cal. 2017); *Amazon.com v. Lay*, 758 F. Supp. 2d 1154, 1170 (W.D. Wash. 2010). The legislative history of the VPPA "confirms that Congress was concerned with protecting the confidentiality of private information about viewing preferences *regardless of the business model* or media format involved." *Hulu*, 2012 WL 3282960, at *6 (emphasis added); *see also Nickelodeon II*, 827 F.3d at 286 ("If, for example, Google were to start purposefully leaking its customers' YouTube video-watching histories, we think such disclosures would almost certainly violate the Act.").

Facebook's arguments that it is not covered by the VPPA fail. First, Facebook argues that

it does not "deliver" videos, MTD 36, despite that over 8 billion videos a day are viewed on Facebook. ¶ 309. This Court has appropriately questioned Facebook's interpretation, noting that "'delivery' means something other than rental or sale," and Facebook appears to be "reading the word 'delivery' out of the statute." Tr. of Proceedings 173:1-2, 178:24-179:3, Feb. 1, 2019. Facebook's own authority confirms this is so.[27] Likewise, Facebook's suggestion that "delivery" should be limited to commercial, monetary "transaction[s]" should not be credited.[28] Plaintiffs allege that they "entered into transactions with Facebook" for, *inter alia*, "the purpose of subscribing to Facebook's video streaming content and services," and Plaintiffs allege that the users' content has monetary value. ¶ 866; *see also, e.g.*, ¶ 292. Facebook's contention that the VPPA applies only to "the video-rental stores of the 21st century" such as "Block[buster] or its mode[rn] equivalents" is wrong. *Cf.* MTD 35-36.

Second, Facebook argues that it is only "peripherally" involved in video services, and that this is not a "core" part of its business. MTD 35. To the contrary, Facebook is substantially involved in video delivery, and significantly tailored its business to this purpose by (1) creating a platform to upload, share, like, and comment on videos through Facebook and Facebook Messenger; (2) developing infrastructure to store and deliver uploaded and shared videos, including depositories that "cache" videos for delivery to users; (3) enabling access to video-related content and information through API feeds; (4) advertising video as a core component of its platform; and (5) "enter[ing] into agreements with content providers" to enable its users to access their content. *See* ¶¶ 307-09, 416-52, 862, 864.[29] Thus, video delivery is a key part of

[27] *Vizio*, 238 F. Supp. 3d at 1221 ("Congress's use of a disjunctive list (*i.e.*, 'engaged in the business . . . of . . . rental, sale, *or* delivery') unmistakably indicates that Congress intended to cover more than just the local video rental store"—"lest the word 'delivery' be superfluous, a person need not be in the business of either renting or selling video content for the statute to apply.") (citation omitted).

[28] *See Hulu*, 2012 WL 3282960, at *7 (VPPA claim does not require plaintiffs to "allege that they rented or purchased content" from defendant, nor does it require "payment" or "exchange of money"); *cf.* MTD 36; Tr. of Proceedings 178:24-179:11, Feb. 1, 2019.

[29] The examples considered by the *Vizio* court are not analogous to Facebook: a "letter carrier who physically places a package that happens to contain a videotape into a consumer's mailbox," "Blu–Ray players, smartphones, app stores, cable boxes, wireless routers, personal computers, video game consoles, [or] even cars." *Vizio*, 238 F. Supp. 3d at 1221-22.

Facebook's platform as well as its efforts to maintain user engagement.[30] It is also a cornerstone of Facebook's monetization of Plaintiffs' private content.

b. Facebook Disclosed "Personally Identifiable Information."

Under the VPPA, PII "includes information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider." 18 U.S.C. § 2710(a)(3).[31] For example, Facebook does not dispute that the "read_mailbox" API category disclosed information regarding videos that Plaintiffs obtained through Facebook Messenger. Likewise, through the "read_stream" API category, Facebook disclosed "any videos uploaded by the user as well as any videos or video hyperlinks shared with a user." ¶¶ 423, 462. This includes both "video materials and services" that users "requested or obtained" because sharing a video reflects that it has been obtained from Facebook, through its ten data centers created for that purpose. ¶ 417. Facebook thus obtained Plaintiffs' PII, in that "[o]n or through Facebook, Facebook Messenger, and/or Facebook Chat," Plaintiffs have "watched videos, 'liked' videos, 'shared' videos, 'posted' videos, 'liked' pages on Facebook that contain videos, and 'shared' pages on Facebook that contain videos."[32] Likewise, Plaintiffs allege that Facebook disclosed their PII through at least twelve different API categories. ¶¶ 419-25, 867.[33] This PII "identified Plaintiffs as having 'requested or obtained specific video materials or services,'" and "included Facebook user IDs, names, addresses as well as information about Plaintiffs' downloads, views, and comments relating to the videos that Facebook delivered," as well as "posts of videos, other video-related posts, Likes of videos, Page Likes for videos, tags in videos, video-related actions

[30] ¶¶ 416-52, 862, 864; *see Vizio*, 238 F. Supp. 3d at 1221-22 (defendant in the "business" of delivering video content, because it "developed a product intimately involved in the delivery of video content to consumers," and had "created a supporting ecosystem to seamlessly deliver video content to consumers," including "entering into agreements with content providers").

[31] Facebook argues that "[t]he definition of personally identifiable information 'is intended to be transaction-oriented,' and limited to 'information that identifies a particular person as having engaged in a specific transaction,'" MTD 36, but does not dispute that this transaction is "request[ing] or obtain[ing] specific video materials or services," 18 U.S.C. § 2710(a)(3).

[32] ¶¶ 27, 35, 43, 51, 60, 68, 77, 85, 93, 101, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 187, 194, 202, 210, 218, 226, 234, 242, 245, 253, 256.

[33] Facebook does not contend that the friends_actions_video, friends_photo_video_tags, and friends_status API categories did not disclose Plaintiffs' PII. ¶ 867; *cf.* MTD 37 n.20.

such as commenting on videos and sharing videos delivered by Facebook to News Feed and on users' Timelines, and messages containing videos all revealed that users had requested or obtained video content." ¶ 868. These include videos shared in non-public forums subject to Privacy Settings. These allegations are more than sufficient to deny dismissal under Rule 12(b)(6) because they "identif[y] a person as having requested or obtained specific video materials or services from" Facebook.

Facebook argues that Plaintiffs do not allege that it "revealed videos that a user actually watched on Facebook." MTD 37. This misstates the standard. The VPPA does not require videos to be "actually watched."[34] Even the fact that a customer rented a video does not indicate that the customer actually watched the video, only that he or she "requested" or "obtained" it. *See In re Nickelodeon Consumer Privacy Litig.*, 2014 WL 3012873, at *10 (D.N.J. July 2, 2014) ("PII is information which must, without more, itself *link an actual person to actual video materials*.") (emphasis added). This distinction alone is dispositive. For example, Facebook does not dispute that the "read_mailbox" API category disclosed information regarding videos that Plaintiffs obtained through Facebook Messenger. Further, Facebook does not dispute that it disclosed Plaintiffs' "comments relating to the videos that Facebook delivered," which clearly identify videos that Plaintiffs viewed, "requested or obtained." ¶¶ 419, 436, 868. Facebook ignores the allegation that it disclosed Plaintiffs' "Likes of videos" (as distinct from "Page Likes for videos"). ¶ 868. Facebook also fails to meaningfully address its disclosure of information through the "read_stream" API category for videos Plaintiffs obtained through their News Feed, ¶¶ 417, 423, 462, relying on the same false premise that the videos must actually be viewed on Facebook. All of these well pleaded facts satisfy the VPPA.

3. Facebook Violated the Stored Communications Act.

Plaintiffs properly plead that Facebook violated Sections 2702(a)(1) and 2702(a)(2) of

[34] Facebook's authorities concern scenarios where it could not be determined from the data that a customer obtained or requested specific videos. *See Nickelodeon II*, 827 F.3d at 283 (concerning an IP address or a digital code in a cookie file); *Gonzalez v. Cent. Elec.*, 2009 WL 3415235, at *11 (D. Or. Oct. 15, 2009) (concerning prices that could be applicable to any one of fifteen titles).

the SCA by knowingly divulging the contents of Plaintiffs' electronic communications to unauthorized parties that were (a) carried and maintained by Facebook, and (b) in electronic storage. ¶¶ 829-58. Facebook does not contest that the SCA applies or that it knowingly divulged the contents of Plaintiffs' electronic communications. Its remaining arguments fail.

To begin with, as discussed in Section III.B.2 above, Plaintiffs did not consent to Facebook's distribution of their personal information to App developers, Whitelisted Apps, and Business Partners, through Friends. Similarly, Facebook's argument that Friends consented to the disclosures of Plaintiffs' content and information is meritless. MTD 33-34. "[A]s the party seeking the benefit of the exception" under the SCA, Facebook bears the burden of demonstrating consent—which here it has failed to do. *See Matera*, 2016 WL 5339806, at *17.[35] Here, Plaintiffs clearly allege that App users "were not aware of and did not consent to the disclosure" of the "electronic communications of their Friends or the Friends of their Friends to unauthorized parties, including Cambridge Analytica, Business Partners, other advertisers, and data brokers," as is detailed further in Section III.B.2, above. ¶ 853. Similarly, App users did not consent to disclosure to advertisers or any other disclosure or use "beyond the App" itself. *Id.*

Moreover, the SCA's lawful consent exception "is not satisfied by consent that is merely constructive, implied in law, or otherwise *imputed* to the user by a court," but rather requires "the user's actual consent." *Negro v. Superior Court*, 230 Cal. App. 4th 879, 889 (2014) (emphasis in original). Facebook fails to point to allegations supportive of its claim that Friends—including users of the This Is Your Digital Life App—actually and knowingly consented to the wholesale disclosure and harvesting of the contents of their Friends' electronic communications. Facebook's claims especially strain credulity with respect to Whitelisted Apps, which Facebook allowed to "access user data without permission" and which could "circumvent users' privacy [or] platform settings and access Friends' information, even when the user disabled the Platform," as well as with respect to Business Partners, which Facebook allowed "to hide their

[35] Although *Matera* involved Wiretap Act claims, the "consent" exceptions to liability under the Wiretap Act and the SCA (separate sections of the Electronic Communications Protection Act) are analogous. *Perkins*, 53 F. Supp. 3d at 1211-12.

access from users and to share information even where users expressly attempted to prevent this access." ¶¶ 496, 563, 602. The cases cited by Facebook do not support its position. Where communications are "configured to be accessible to only specific recipients," they cannot be disclosed without clear consent.[36] Cases applying the SCA's lawful consent exception involve actual, knowing consent.[37] Congress intended to limit the scope of the lawful consent exception.[38] Facebook has failed to meet its burden.

The SCA sets forth statutory minimum damages of $1,000, though a court may assess "the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation." 18 U.S.C. § 2707(c). Here, Plaintiffs allege actual damages, as discussed in Section III.A.2 above. Facebook has also profited from its violations of the SCA, in that "sharing user content and information with third parties was enormously valuable to Facebook," ¶ 295, and "Facebook's sharing of user content and information with third parties—including Apps, Business Partners, Whitelisted Apps, and advertisers—has resulted in 'explosive revenue growth.'" ¶ 296; *see also* ¶ 855. The cases cited by Facebook involving SCA claims expressly provide that *either* actual damages or profits made by the violator are required for statutory damages to apply.[39] *Van Alstyne* expressly provides that punitive damages (as well as attorneys' fees) may be awarded, even in the absence of actual damages. 560 F.3d at 209 (upholding the

---

[36] *See Facebook v. Superior Court* ("*Facebook II*"), 4 Cal. 5th 1245, 1276 (2018) (rejecting Facebook's argument that implied consent under section 2702(b)(3) should be "triggered" by communications "configured by the user to be *restricted*, but nonetheless accessible to a 'large group' of friends or followers"); *In re Facebook*, 923 F. Supp. 2d 1204, 1205-06 (N.D. Cal. 2012) (granting Facebook's motion to quash subpoena "on the grounds that the subpoena violates the Stored Communications Act").

[37] *See, e.g.*, *Negro*, 230 Cal. App. 4th at 883-84, 899 (express consent provided by email sufficient to satisfy the SCA's lawful consent exception); *Gen. Elec. v. Liang*, 2014 WL 12844840, at *1 (C.D. Cal. Aug. 25, 2014) (defendant "executed a consent directive consistent with the SCA"); *Super Vitaminas*, 2017 WL 5571037, at *4 (N.D. Cal. Nov. 20, 2017) (SCA not violated where declarations were submitted by addressees of the communications).

[38] *See Facebook II*, 4 Cal. 5th at 1278 ("The legislative history suggests that Congress intended to exclude from the scope of the lawful consent exception communications configured by the user to be accessible to only specified recipients.").

[39] *Vista Mktg. v. Burkett*, 812 F.3d 954, 966 (11th Cir. 2016); *Van Alstyne v. Elec. Scriptorium*, 560 F.3d 199, 205 (4th Cir. 2009).

district court's award of punitive damages). Thus, where—as here—it is alleged that "Defendants' violations of the SCA were committed willfully and intentionally," ¶ 858, punitive damages and attorneys' fees may be awarded even in the absence of actual damages or profits. In contrast, the cases cited by Facebook involve factual findings that there were no actual damages or profits received.[40]

Facebook's remaining contentions are similarly meritless. Facebook's arguments regarding "Plaintiffs' 'indirect disclosure' theory," MTD 34, are bereft of legal support and should not be credited. Facebook cites *Freeman v. DirecTV*, 457 F.3d 1001, 1004 (9th Cir. 2006), MTD 34, in which neither defendant was a stored communications provider. The issue was whether the SCA "creates a private right of action for conspiracy or aiding and abetting." *Freeman*, 457 F.3d at 1004. Here, Facebook is an electronic communications service provider subject to primary liability under the SCA. ¶¶ 829-58. Facebook directly disclosed the contents of Plaintiffs' electronic communications to the This Is Your Digital Life App as well as thousands of other Apps, Whitelisted Apps, Business Partners, and advertisers. *See* ¶¶ 847-48; *see also* ¶¶ 33, 41, 49, 58, 66, 74, 83, 91, 99, 102, 110, 118, 126, 134, 142, 150, 158, 166, 174, 182, 185, 192, 200, 208, 216, 223, 232, 240, 243, 251, 254, 262. Finally, it is demonstrably false that Plaintiffs *only* allege disclosure to the This Is Your Digital Life App. *See* ¶¶ 406-11, 847-48. Even if this were so, the allegations are nevertheless sufficient to state a claim under the SCA. *See* 18 U.S.C. § 2702(a)(1)-(2).

F. The FAC Adequately Pleads Violations of Plaintiffs' Privacy.

1. Facebook's Challenges to Plaintiffs' Privacy Claims Under the California Constitution and for Intrusion into Private Affairs Are Unavailing.

Facebook challenges Plaintiffs' claims for invasion of privacy by intrusion into private affairs and for violation of Article I, Section I of the California Constitution, arguing that Plaintiffs "consented to disclosure" and so have no reasonable expectation of privacy. MTD 41.

[40] *See Vista Mktg.*, 812 F.3d at 957 (jury did not award actual or punitive damages); *Van Alstyne*, 560 F.3d at 209 (jury did not award actual damages); *see also Doe v. Chao*, 540 U.S. 614, 617 (2004) (as to Privacy Act claim, which does not involve consideration of profits made by the violator, summary judgment granted where there were "no issues of cognizable harm").

As set forth in Section III.B.2 above, Facebook's arguments about consent should be rejected.

Facebook contends that Plaintiffs have not demonstrated a legally protected privacy interest because "Plaintiffs allege only categories of information that were shared." MTD 41. Not so. Plaintiffs allege that Facebook disclosed private content and information, including personal and family photographs and videos, location information, personal perspectives and private messages regarding politics, religion, relationships, work, health, and family. ¶¶ 30, 38, 46, 54, 55, 63, 71, 80, 88, 96, 107, 115, 123, 131, 139, 147, 155, 163, 171, 179, 190, 197, 205, 214, 221, 229, 237, 248, 259. This is exactly the sort of "sensitive and confidential information" courts deem protected.[41] Facebook's misconduct encompasses "the principal 'mischiefs' at which [Article I, Section I of the California Constitution] is directed," including "the overbroad collection and retention of unnecessary personal information by government and business interests," and "the improper use of information properly obtained for a specific purpose, for example, the use of it for another purpose or the disclosure of it to some third party." *White v. Davis*, 13 Cal. 3d 757, 775 (1975). The cases cited by Facebook are readily distinguishable because, here, Plaintiffs have alleged more than "enough detail for the Court to determine whether it might conceivably fall within a recognized privacy interest."[42]

Facebook's conduct is "sufficiently serious" to constitute an "egregious breach of social norms" under Article I, Section I of the California Constitution. Facebook not only violated Plaintiffs' privacy interests, but also misled Plaintiffs into believing that it would protect their privacy choices. *See, e.g.*, *Google Cookie Placement*, 806 F.3d at 150-51. As in *Google Cookie*

[41] *See, e.g.*, *Hughey v. Drummond*, 2015 WL 4395013, at *11-12 (E.D. Cal. July 16, 2015) (finding a legally protected privacy interest in materials containing "personal family photos and other personal electronic files"); *Facebook v. Superior Court* ("*Facebook I*"), 15 Cal. App. 5th 729, 738 (2017) (analogizing Facebook posts to private holiday greeting cards, which may inform friends and relatives "of highly personal events such as births, deaths, illness or job loss" and may include "personal photographs").

[42] *Scott-Codiga v. Cty. of Monterey*, 2011 WL 4434812, at *6-7 (N.D. Cal. Sept. 23, 2011) (alleging only disclosure of unspecified work-related information by email); *see also In re Yahoo Mail Litig.*, 7 F. Supp. 3d 1016, 1041 (N.D. Cal. 2014) (conclusory allegation that emails were "private"); *Zbitnoff v. Nationstar Mortg.*, 2014 WL 1101161, at *4 (N.D. Cal. Mar. 18, 2014) (alleging unspecified "private information" disclosed to unspecified third parties).

Placement, Facebook promised not to share users' private content and information with advertisers and other third parties, when, in fact, Facebook engaged in its wholesale disclosure to third parties—including advertisers—profiting enormously as a result. *See* ¶¶ 603-06. Likewise, Facebook promised that users could "control who can see your information," "control how it is shared," and that Facebook would "mak[e] sure only those people [users] intend can see it." ¶ 723; *see also* ¶¶ 593-94. This was false. Facebook gave Business Partners and Whitelisted Apps wholesale access to Plaintiffs' private content and information. *See* ¶¶ 496, 515, 595, 600-02, 680. Facebook's disclosure of Plaintiffs' content and information to third parties for its own benefit, at the expenses of its users, constitutes an egregious breach of Plaintiffs' right to privacy. *Google Cookie Placement*, 806 F.3d at 150-51; *see also Goodman*, 2012 WL 2412070, at *1, *15 (allegations that defendant used location tracking data to "analyze [plaintiffs'] behavior, build profiles about them, and sell this information to third parties" were sufficient to find "a serious invasion of a protected privacy interest" and "an egregious breach" of social norms).[43] The cases cited by Facebook are inapposite, because they do not address the wealth of information Facebook disclosed, its affirmative misrepresentations regarding privacy, or that it disclosed content and information that Plaintiffs specifically designated as non-public.[44]

Plaintiffs have clearly alleged conduct that would be "highly offensive to a reasonable person," for purposes of their common-law privacy claims. In determining "offensiveness," courts examine "the degree of the intrusion, the context, conduct and circumstances surrounding the intrusion as well as the intruder's motives and objectives, the setting into which he intrudes, and the expectations of those whose privacy is invaded." *Miller v. Nat'l Broad. Co.*, 187 Cal. App. 3d 1463, 1483-84 (1986); *Opperman*, 205 F. Supp. 3d at 1077. Here, every factor weighs in

[43] Plaintiffs allege that Facebook disclosed fine location data, such as that "associated with smartphones and other mobile devices," without consent. ¶¶ 1264-68.

[44] *See Folgelstrom v. Lamps Plus*, 195 Cal. App. 4th 986, 992 (2011) (defendant's request for ZIP code to obtain mailing address "routine commercial behavior"); *In re Yahoo Mail Litig.*, 7 F. Supp. 3d at 1039 (insufficient facts to determine whether defendant invaded plaintiffs' constitutional right of privacy); *Razuki v. Caliber Home Loans*, 2018 WL 2761818, at *2 (S.D. Cal. June 8, 2018) (negligent failure to protect consumer data not an egregious breach of social norms).

Plaintiffs' favor. Facebook disclosed Plaintiffs' highly personal information, including private messages, location information, and personal and family photographs and videos; it did so despite Plaintiffs' express designation of such information as non-public; Facebook concealed from and misled Plaintiffs regarding its data sharing; it intruded into a space in which Plaintiffs shared sensitive personal information; and Facebook acted for its own commercial benefit. ¶¶ 494-96, 517, 680, 806. Moreover, the "intense public outcry and numerous, international governmental investigations" confirm that Facebook's conduct constitutes both an "egregious breach of social norms" as well as conduct "highly offensive to a reasonable person." ¶ 1001.

2. Plaintiffs State a Claim for Public Disclosure of Private Facts.

Facebook invaded Plaintiffs' right to privacy by publishing their private content and information. In *Kinsey v. Macur*, 107 Cal. App. 3d 265 (1980), the California Court of Appeal found the "mailing of letters to 'perhaps twenty [people] at most'" sufficient to justify a claim for public disclosure of private facts. *Id.* at 271-72. The court reasoned that the recipients of the letters "comprised a diverse group of people living in several states and totally unconnected either socially or professionally," and that the group "adequately reflect[ed] 'mass exposure.'" *Id.* at 272. Therefore, a claim for public disclosure of private facts is not "one of total secrecy," rather "it is the right to *define* one's circle of intimacy." *Id.* (emphasis in original). Here, Plaintiffs shared this content and information with a non-public audience and did not intend for it to be viewed by third parties. Despite this, Facebook published Plaintiffs' content and information to dozens of Business Partners, thousands of Whitelisted Apps, and tens of thousands of Apps used by Friends. ¶¶ 472, 484, 497, 930. Thus, Plaintiffs sufficiently allege public disclosure.[45]

Facebook's remaining arguments regarding the specificity of what data and facts were

[45] Facebook's reliance on *Del Llano v. Vivint Solar* (MTD 42) is misplaced. There, the plaintiff did not allege disclosure or release of private information at all. 2018 WL 656094, at *5 (S.D. Cal. Feb. 1, 2018). Facebook also mistakenly relies on *Moreno v. Hanford Sentinel*, 172 Cal. App. 4th 1125 (2009) where plaintiff, by publicly posting to Myspace, "opened [her article] to the public eye." 172 Cal. App. 4th at 1130. Unlike *Moreno*, Plaintiffs did not make their content and information available to the public at large.

shared as well as the "egregious[ness]" of Facebook's publication should be rejected for the reasons set forth in Sections III.A.1 and III.F.1 above, respectively. MTD 42.

3. Facebook Violated Plaintiffs' Right of Publicity.

Facebook violated Plaintiffs' right of publicity by appropriating Plaintiffs' names and likenesses for commercial or other advantage. *See Eastwood v. Superior Court*, 149 Cal. App. 3d 409, 417 (1983). Here, Facebook bartered Plaintiffs' names and likeness to thousands of Whitelisted Apps for value, including advertising revenues. ¶¶ 303, 502, 511. Similarly, Facebook traded Plaintiffs' names and likeness to a diverse set of Business Partners to promote and expand Facebook's Platform across devices, websites, and service providers in exchange for similar data from these partners as well as advertising revenues. ¶¶ 291, 486, 487, 710. Facebook also made Plaintiffs' names and likeness available to third parties, including Cambridge Analytica, which in turn purchased targeted advertisements on Facebook using the personal information disclosed by Facebook. ¶ 754. Facebook gained commercial advantage by making Plaintiffs' names, likenesses, and other personal information available to third parties. ¶¶ 290-97. The cases cited by Facebook are not to the contrary.[46]

G. Facebook Committed Fraud by Omission.

Facebook committed fraud by omission within the meaning of California Civil Code § 1710(3), which defines fraud as "[t]he suppression of a fact, by one who is bound to disclose it, or who gives information of other facts which are likely to mislead for want of communication of that fact." Because Facebook willfully deceived Plaintiffs with the intent to induce them to alter their position to their injury or risk, Facebook "is liable for any damage which [Plaintiffs] thereby suffer[ed]." ¶¶ 877-911; *see* Cal. Civ. Code § 1709.

For instance, Facebook's SRR promised users that "[w]e do not give your content or information to advertisers without your consent," ¶ 603, which gave rise to an obligation that Facebook disclose, *inter alia*, that it allowed advertisers that were Apps, Whitelisted Apps, or

[46] *Goodman*, 2012 WL 2412070, does not involve a right of publicity claim, and *Timed Out v. Youabian*, 229 Cal. App. 4th 1001, 1008 (2014), stands for the proposition that common law right of privacy claims are assignable.

Business partners "to access users' content." ¶¶ 605-06. Likewise, Facebook concealed from users the existence of the Whitelisted Apps and Business Partners programs, which Facebook was obligated to disclose, because it promised users that "[y]ou own all of the content and information you post on Facebook, and you can control how it is shared through your privacy [hyperlinked] and application [hyperlinked] settings," ¶ 593, and it made statements promising users control of personal information. ¶¶ 284, 721-46. These affirmative statements gave rise to an obligation that Facebook disclose:

- that "users had *no* control over whether and how their content and information was shared with Business Partners," ¶ 595; *see also* ¶ 602; and
- that Facebook allowed Whitelisted Apps "to continue to access Friends' data even after users attempted to disable" such access, ¶¶ 599-600; *see also* ¶ 601.

As detailed in Section III.B.2, Facebook had a duty to disclose these and other facts to Plaintiffs, based on, *inter alia*, the highly sensitive nature of the content and information that Facebook obtained from Plaintiffs and unlawfully shared with third parties. *See* ¶¶ 885, 896, 901, 954.

Facebook committed deceit in two other ways. First, Facebook was aware of known security risks that jeopardized the security of Plaintiffs' content, and knowingly failed to take action in response to warnings it had received. ¶¶ 536-74, 690, 770, 881. In light of the promises Facebook made about privacy and control, Facebook had a duty to disclose the risk that Plaintiffs' content and information would be obtained by unauthorized parties. *See In re Yahoo! Inc. Customer Data Sec. Breach Litig* ("*Yahoo! II*"), 313 F. Supp. 3d 1113, 1133-34 (N.D. Cal. 2018) ("[T]he importance of Defendants' security measures [was] a factor in Plaintiffs' decision whether to use Defendants' services" and, "had [plaintiffs] known about the inadequacy of these security measures, they 'would have taken measures to protect themselves.'") (citation omitted). Second, contrary to its statement that "[a]dvertisers never get access to your information," ¶ 734, Facebook allowed Plaintiffs' content and information to be deanonymized, linked with other sources such as data brokers, and used to individually target Plaintiffs with psychographic advertisements. ¶¶ 315-21, 457, 619-20, 751-77.

Facebook fails to provide substantive support for its conclusory assertions that Plaintiffs

"do not allege any personal injury," and "have not suffered any damages," and has waived these arguments. MTD 39-40.[47] So too has Facebook failed to support and therefore waived the argument that Plaintiffs "have not pled fraudulent concealment with particularity under Rule 9(b)." MTD 39.[48] Finally, Facebook's argument regarding the purported "waiver of liability for third-party actions" should be rejected for the reasons set forth above in Section III.D.

H. Facebook Violated the Unfair Competition Law ("UCL").

Plaintiffs allege that they are entitled to restitution, because they entrusted Facebook with their personal content and information subject to privacy restrictions; Plaintiffs were harmed when Facebook violated those Plaintiffs' Privacy Settings and took more content than they were entitled to; and Facebook wrongfully monetized and profited from the taking. ¶¶ 778-801, 982-91.[49] Entitlement to restitution is sufficient to demonstrate a loss of money or property under the UCL and also satisfies Article III standing. *Anthem II*, 2016 WL 3029783, at *30. As addressed in Section III.A.2, Plaintiffs suffered economic injury as a result of Facebook's unfair competition. *See Kwikset v. Superior Court*, 51 Cal. 4th 310, 323 (2011); *Witriol v. LexisNexis*, 2006 WL 4725713, at *1, *6 (N.D. Cal. Feb. 10, 2006).

Facebook's reliance on *In re Sony Gaming Networks and Customer Data Sec. Breach Litig.*, 903 F. Supp. 2d 942 (S.D. Cal. 2012), is misplaced. The *Sony* court dismissed plaintiffs' UCL claim because "Sony did not benefit financially from the Data Breach." *Id*. at 970. Here,

---

[47] *Tenet Healthsystem Desert v. Blue Cross of Cal.*, 245 Cal. App. 4th 821, 844 (2016), does not support Facebook's proposition. Plaintiffs adequately allege injury and damages, as detailed above in Section III.A. Further, Plaintiffs allege "emotional distress," ¶¶ 34, 42, 50, 59, 67, 76, 92, 100, 103, 111, 119, 127, 135, 143, 151, 159, 167, 175, 183, 186, 193, 201, 209, 217, 225, 233, 241, 244, 252, 255, 263, and "damages for mental pain and suffering are recoverable in a tort action of deceit," *Sprague v. Frank J. Sanders Lincoln Mercury*, 120 Cal. App. 3d 412, 417 (1981). Also, "one may recover compensation for time and effort expended in reliance on a defendant's misrepresentation," as Plaintiffs have alleged. ¶ 791; *see Block v. Tobin*, 45 Cal. App. 3d 214, 220 (1975).

[48] *See Yahoo! II*, 313 F. Supp. 3d at 1134 ("Defendants argue that Plaintiffs must provide more detail about Defendants' omissions," but "offer no explanation of what more Plaintiffs need to identify.").

[49] Facebook falsely suggests that Plaintiffs are seeking damages under the UCL. MTD 45; *see* ¶¶ 991-92 (Plaintiffs seek restitution and injunctive relief).

Facebook has profited enormously from its wrongdoing. *See id.* (restitution is "appropriate even where defendant did not receive money directly from plaintiff if defendant otherwise profited from an unfair business practice"); *Google Android II*, 2014 WL 988889, at *7. Likewise, in *Korea Supply v. Lockheed Martin*, the "plaintiff [did] not have an ownership interest in the money it seeks to recover from defendants." 29 Cal. 4th 1134, 1149 (2003). Here, Plaintiffs allege a "property interest in Facebook's profits." ¶¶ 982, 991.

Plaintiffs adequately plead claims under all three prongs of the UCL. Plaintiffs plead both statutory and constitutional violations, and thus plead a UCL claim under the "unlawful" prong. *See, e.g.*, ¶¶ 829-911, 969-1006; *In re Yahoo! Inc. Customer Data Sec. Breach Litig*. ("*Yahoo! I*"), 2017 WL 3727318, at *23 (N.D. Cal. Aug. 30, 2017). As detailed in Section III.G, Plaintiffs allege deceitful conduct and fraudulent omission, which serves as the basis of a UCL claim under the "fraudulent" prong. *Yahoo! I*, 2017 WL 3727318, at *24, *29-30; *see also* ¶¶ 979, 982, 988-89. Likewise, Plaintiffs allege a claim under the "unfair" prong, in that Facebook violated California's strong public policy of protecting privacy interests, and Facebook externalized the costs of protecting users' personal information, requiring Plaintiffs to take independent action to protect themselves.[50] *See* ¶¶ 778-801, 973, 975; *In re Anthem Data Breach Litig.*, 162 F. Supp. 3d 953, 989-90 (N.D. Cal. 2016); *In re Adobe Sys. Privacy Litig.*, 66 F. Supp. 3d 1197, 1227 (N.D. Cal. 2014); *iPhone II*, 844 F. Supp. 2d at 1073.

I. Plaintiffs May Maintain Their Claim for Unjust Enrichment.

The Complaint alleges both that Plaintiffs rendered services to Facebook's benefit and that Facebook would be unjustly enriched if Plaintiffs were not compensated. ¶¶ 289, 292-97, 303, 330-34, 487, 498, 744, 1034-42; *see Precision Pay Phones v. Qwest Commc'ns*, 210 F. Supp. 2d 1106, 1112 (N.D. Cal. 2002). These allegations are unchallenged.

Facebook argues only that "Plaintiffs concede that they 'agreed on express terms'

[50] Facebook wrongly argues that claims under the "unfair" prong are limited to competition claims. MTD 45 (citing *Durell v. Sharp Healthcare*, 183 Cal. App. 4th 1350, 1366 (2010)). The unfairness prong need concern a harm to competition directly only "in the context of an unfair competition claim by *a competitor*." *Durell*, 183 Cal. App. 4th at 1364.

governing their claims." MTD 45. However, Plaintiffs plead their claim for unjust enrichment in the alternative to breach of contract, and courts routinely allow both express contract and implied contract theories to proceed past the motion to dismiss stage. ¶ 1033; *see Yahoo! I*, 2017 WL 3727318, at *47-48; *Stitt v. Citibank*, 942 F. Supp. 2d 944, 960 (N.D. Cal. 2013); *Ellis v. J.P. Morgan Chase & Co.*, 950 F. Supp. 2d 1062, 1091 (N.D. Cal. 2013). Plaintiffs seek compensation for uses of content and information that are not addressed by any contract, such as the substantial revenues Facebook received from Whitelisted Apps. ¶ 1037.

J. Plaintiffs State a Claim for Negligence and Gross Negligence.

Facebook's principal argument against Plaintiffs' negligence-based claim is that it owed them no duty of care. This is incorrect.[51] California has long recognized a duty of care owed by a defendant from transactions involving third parties, even if the plaintiff suffers only economic loss. *See, e.g., Yahoo! II*, 313 F. Supp. 3d at 1132-33. Plaintiffs do *not* ground that duty in the contracts between Facebook and Plaintiffs. Rather, they allege that they "entrusted [Facebook] with their content and information, which provided an independent duty of care." ¶ 954.

To determine whether Facebook owes a duty for Plaintiffs' economic losses, California law looks to the six *J'Aire* factors. *See Yahoo! II*, 313 F. Supp. 3d at 1132 (citing *J'Aire v. Gregory*, 24 Cal. 3d 799, 804 (1979)). In applying the first *J'Aire* factor, the extent to which the transaction was intended to affect the plaintiff, California law examines the "primary purpose" of the transaction. *Centinela Freeman Emergency Med. Assocs. v. Health Net of Cal.*, 1 Cal. 5th 994, 1015 (2016). Here, the primary purpose of the transaction between Facebook and third-party Apps, websites, and Business Partners was to provide access to Plaintiffs' content and information. *See, e.g.*, ¶¶ 442, 486-87 497, 503, 710(d). Facebook is wrong to claim that Plaintiffs *alone* must have been intended to be affected by a transaction. MTD 43. Plaintiffs need only be—and are—members of "a class" intended to be affected. *Centinela*, 1 Cal. 5th at 1014

[51] To the extent Facebook asserts express or implied consent as a defense to its conduct, it errs. Even if Plaintiffs had consented to all that Facebook claims, they did not consent to Facebook's negligence. It is assumption of risk, not consent, that is a relevant defense to Plaintiffs' negligence claim, but Facebook does not assert that defense in its Motion. *See* Restatement (Second) of Torts § 892 cmt. a (1979).

n.10.

Facebook argues that the closeness of connection factor favors no duty, citing Plaintiffs' purported focus on the acts of third parties. MTD 44. Yet Plaintiffs challenge *Facebook's* knowledge that it was disseminating sensitive information, not a third party's knowledge. Facebook has admitted it "should have been doing more all along" to audit third parties. ¶ 729. Facebook argues that the risk of future harm is minimal, but Facebook has not changed its approach of "willful blindness" to Apps' data misuse, and has conducted no audit of Business Partners that continue to receive access.[52] ¶¶ 555, 562. Facebook raises almost no challenge to the foreseeability, degree of certainty, and moral blame *J'Aire* factors, other than to argue Plaintiffs suffered no harm. Not so. *See* Section III.A.

Citing inapposite cases, Facebook maintains that it owes no duty of care to Plaintiffs. *See* MTD 43 (citing *In re Google Android Consumer Privacy Litig.* ("*Google Android I*"), 2013 WL 1283236, at *13 (N.D. Cal. Mar. 26, 2013); *Pirozzi v. Apple, Inc.*, 913 F. Supp. 2d 840, 852 (N.D. Cal. 2012); *In re iPhone Application Litig.* ("*iPhone I*"), 2011 WL 4403963, at *9 (N.D. Cal. Sept. 20, 2011)). In each, purchasers of smartphones asserted that the phone maker owed them a duty to prevent applications available at Apple's app store or Google's Android Market from wrongly taking the purchasers' personal information. Here, Plaintiffs' negligence claims do not rely simply on Facebook's status as developer of a platform. Third parties obtained users' sensitive information from Facebook, which had been entrusted with such information. Moreover, Facebook knew for years that its users' content was vulnerable, but did nothing. ¶¶ 536-62; *see Yahoo! II*, 313 F. Supp. 3d at 1131-32 (holding that negligence claim satisfied *J'Aire* because Yahoo! knew of specific security risks and took no action).[53]

[52] *See supra* note 7, reporting that 540 million records of Facebook users' content and information that Facebook made available to third-party developers were recently found on Amazon's cloud servers.

[53] Facebook's authorities deal with manufacturers and retail customers, or do not address a special relationship, and thus are inapposite. MTD 43-44; *Greystone Homes v. Midtec*, 168 Cal. App. 4th 1194, 1230-31 (2008) (plumbing fitting manufacturer); *Platte Anchor Bolt v. IHI*, 352 F. Supp. 2d 1048, 1055 (N.D. Cal. 2004) (supplier to subcontractor).

K. In the Alternative to Quasi-Contract, Facebook Breached the Terms of the Contracts.

1. Plaintiffs Have Standing to Pursue a Breach of Contract Claim.

Plaintiffs have Article III standing to pursue a breach of contract claim even if they have not suffered economic harm. This is true for two reasons. First, a breach of a contractual promise, even without more, "has traditionally been regarded as providing a basis for a lawsuit in English [and] American courts." *Spokeo*, 136 S. Ct. at 1549. The California Civil Code, enacted in 1872, provides that even if a breach "has caused no appreciable detriment," the party affected "may yet recover nominal damages." Cal. Civ. Code § 3360. This rule has been reaffirmed by the courts. *See, e.g.*, *Sweet v. Johnson*, 169 Cal. App. 2d 630 (1959); *see also* B. Witkin, Summary of California Law: Contracts § 903 (1987). Second, the California Legislature's judgment that a contractual breach is actionable by itself is owed deference. *See Spokeo*, 136 S. Ct. at 1549 (legislative judgment "instructive and important"); *see also Patel*, 290 F. Supp. 3d at 953-54 (deferring to state legislature's view of what constitutes an actionable injury). For these reasons, a breach of an enforceable contractual promise, even without other damage, constitutes an injury in fact. *See In re Facebook Privacy Litig.*, 192 F. Supp. 3d 1053, 1060-62 (N.D. Cal. 2016). *Aguilera v. Pirelli Armstrong Tire*, 223 F.3d 1010 (9th Cir. 2000), cited by Defendants, MTD 44, does not hold otherwise. There, the Ninth Circuit held merely that a breach of contract claim "depends on a showing that they suffered legally cognizable harm" as of the date of breach—which Plaintiffs have shown. *Aguilera*, 223 F.3d at 1015 (declining to recognize fear of future layoff as actionable injury).

2. Facebook Breached Its Promises About Sharing Users' Content and Information and Respecting Users' Privacy.

Facebook promised users that they could control how their content and information was shared using their Privacy or Application Settings. ¶ 593. But Facebook breached this promise when it gave users no control over whether and how Facebook shared their content and information with Whitelisted Apps and Business Partners. ¶¶ 343-44, 375, 383, 595. Likewise, Facebook promised that it would not share users' "content and information with advertisers

without [their] consent." ¶ 604. Despite that promise, Facebook granted third-party App developers and Business Partners access to users' information. ¶¶ 605-06. To the extent that Facebook maintains these third parties are not advertisers, that is false. As Plaintiffs allege, both third-party Apps and Business Partners advertised on Facebook. *Id*. The notion that Facebook did not share data with Apps "*qua* advertisers" is belied by what GSR and Cambridge Analytica did with users' data: they used it for advertising.

The SRR promised that Facebook "require[d] applications to respect your privacy." ¶ 441. But when Facebook made users' photos, videos, checkins, and statuses available, it stripped the privacy designations that users had put on that data. ¶¶ 428-29, 439-40. By making it impossible for applications to "respect" users' Privacy Settings, Facebook breached the SRR.

3. Plaintiffs Have Suffered Damages.

Facebook incorrectly claims that Plaintiffs have not suffered damages from its breach of contract. Plaintiffs contracted to engage on a social platform protected by their own Privacy Settings. They did not receive that service. Rather, they provided to Facebook greater consideration than that for which the parties bargained, where the consideration is access to Plaintiffs' private and otherwise valuable content and information. In addition, Plaintiffs must now accept less privacy than they were promised when they signed up. ¶ 416; *see Fraley*, 830 F. Supp. 2d at 799 (opportunity costs are economic losses); *see also Hinojos v. Kohl's*, 718 F.3d 1098, 1108 (9th Cir. 2013) (noting that "damage" includes opportunity costs and transaction costs).

L. Facebook Breached Its Implied Covenant of Good Faith and Fair Dealing.

Facebook's argument that "Plaintiffs have not alleged contract damages" should be rejected for the same reasons set forth above in Section III.A. Facebook's other substantive challenge is that Facebook's wrongful actions were completely covered by the contract. This is false. For instance, Facebook's promise that it would not "give [users'] content and information to advertisers without [their] consent," ¶ 603, was not "completely covered by the contract," because Facebook's SRR does not address the consequences of Facebook's failure to perform its

contractual obligation. *See also Yahoo! I*, 2017 WL 3727318, at *48 ("Although Defendants did not promise to employ 'specific' cybersecurity measures or 'invest a particular sum of time or money' in cybersecurity, Plaintiffs have sufficiently alleged that Defendants had a contractual duty to employ reasonable safeguards in protecting users' [PII]," and therefore "Plaintiffs have sufficiently alleged an interference with the benefits of the contract for purposes of Plaintiffs' claim under the implied covenant of good faith and fair dealing.").

M. All of Plaintiffs' Claims Are Timely.

Facebook argues that Plaintiffs' claims are time-barred because the FTC Complaint and Consent Decree (together, "FTC Action"), as well as related news coverage,[54] put users on notice "that third-party apps could access user data via permissions from their friends, and that App settings (not Privacy settings) directly controlled how users could limit the sharing of information with apps."[55] MTD 32. But, as noted above in Section III.C.4, the FTC Action, if anything, would have *allayed* users' concerns.

Facebook denied it had engaged in bad practices and repeatedly assured users that their data was secure. Each quarter following the FTC Action, PricewaterhouseCoopers certified that Facebook was in compliance with the Consent Decree. ¶ 550. Until 2018, Facebook "denied that Cambridge Analytica or any of its associated companies had 'Facebook user data'" and stated it had "'no insight on' how Cambridge Analytica may have gathered data from users on Facebook." ¶ 808. Facebook also failed to correct denials by Cambridge Analytica's CEO in testimony before the British Parliament that Cambridge Analytica did not use Facebook users' content and information. ¶¶ 809-11. In any event, the scope of the conduct alleged here was concealed.

---

[54] Plaintiffs object to judicial notice of news articles on grounds other than the existence of the article. *See Khoja v. Orexigen Therapeutics*, 899 F.3d 988, 1003 (9th Cir. 2018).

[55] The FTC Action is not relevant to many of Plaintiffs' *other* allegations. Facebook's assertion that it "did not hide that it had partnerships," MTD 32, does not support its argument. The cited article does not describe the extent of Facebook's data sharing partnerships, nor does it inform users that Facebook's Privacy Controls did not restrict access by Whitelisted Apps to their content and information.

"If a defendant takes active steps to conceal its misdeed, the statute of limitation is tolled until the plaintiff discovers the claim or would have through 'the exercise of reasonable diligence.'" *ShopKo Stores Operating v. Balboa Capital*, 2017 WL 3579879, at *5 (C.D. Cal. July 13, 2017) (citation omitted). Facebook cannot now argue that Plaintiffs should have known it was not telling the truth. *See, e.g., Vucinich v. Paine, Webber, Jackson & Curtis*, 739 F.2d 1434, 1436-37 (9th Cir. 1984) (whether defendant's "reassuring statements" "reasonably affected" when plaintiff was put on notice was "a disputed question of fact").

Plaintiffs could not have learned of the facts through a reasonable investigation where even the FTC did not. Facebook alone knew who was affected and did not tell its users. Because Plaintiffs were not able to discover whether they were injured, they could not have discovered the relevant facts, *Merck & Co. v. Reynolds*, 559 U.S. 633, 653 (2010), or gained "knowledge of the harm," *Jolly v. Eli Lilly & Co.*, 44 Cal. 3d 1103, 1112 (1988).

Facebook also argues that claims relating to the Cambridge Analytica Scandal are time-barred, because of a single 2015 article in *The Guardian*. MTD 32. But, like the FTC Action, the *Guardian* article did not put users on notice about the conduct at issue in this lawsuit, and Facebook makes no showing regarding the *Guardian* article's circulation. *See Eidson v. Medtronic*, 40 F. Supp. 3d 1202, 1221 (N.D. Cal. 2014). The *Guardian* article focuses on Cambridge Analytica's conduct, not on Facebook's. It did not disclose Facebook's routine and widespread dissemination of private content and information. Users, particularly users in the United States who had no dealings with Cambridge Analytica, had no reason to suspect they were affected, especially when Facebook waited until 2018 to tell them.

Accordingly, neither the FTC Action nor the *Guardian* article triggered the limitations period as a matter of California or federal law. *See Merck*, 559 U.S. at 651, 653 ("[W]here the facts would lead a reasonably diligent plaintiff to investigate further . . . the limitations period does not begin to run."); *Fox v. Ethicon Endo-Surgery*, 35 Cal. 4th 797, 808-09 (2005) ("[T]he statute of limitations begins to run on that cause of action when the investigation would have brought such information to light.").

IV. IN THE ALTERNATIVE, PLAINTIFFS SEEK LEAVE TO AMEND

Plaintiffs have standing and state claims for each of the prioritized causes of action in the Complaint. However, in the event the Court dismisses any of these claims, Plaintiffs respectfully seek leave to amend. Under Rule 15(a), leave to amend should be "freely given when justice so requires." *Desertrain v. City of Los Angeles*, 754 F.3d 1147, 1154 (9th Cir. 2014) ("[T]his policy is to be applied with extreme liberality."); *Broam v. Boan*, 320 F.3d 1023, 1028 (9th Cir. 2003) ("Dismissal without leave to amend is proper only in 'extraordinary' cases."). Because the Cambridge Analytica Scandal is ongoing and facts supporting Plaintiffs' claims continue to emerge,[56] if the Court does not uphold any of Plaintiffs' claims, leave to amend should be granted as to any claims that "may be saved by the allegation of additional facts." *See Angelov v. Wilshire Bancorp*, 331 F. App'x 471, 472 (9th Cir. 2009).

V. CONCLUSION

For the reasons set forth above, Plaintiffs ask that the Motion be denied in its entirety.

Dated: April 12, 2019

Respectfully submitted,

KELLER ROHRBACK L.L.P.

By: */s/ Derek W. Loeser*
Derek W. Loeser

Derek W. Loeser (admitted *pro hac vice*)
Lynn Lincoln Sarko (admitted *pro hac vice*)
Gretchen Freeman Cappio (admitted *pro hac vice*)
Cari Campen Laufenberg (admitted *pro hac vice*)
Benjamin Gould (SBN 250630)
1201 Third Avenue, Suite 3200
Seattle, WA 98101
Tel.: (206) 623-1900
Fax: (206) 623-3384

BLEICHMAR FONTI & AULD LLP

By: */s/ Lesley E. Weaver*
Lesley E. Weaver

Lesley E. Weaver (SBN 191305)
Matthew S. Weiler (SBN 236052)
Anne K. Davis (SBN 267909)
Emily C. Aldridge (SBN 299236)
Joshua D. Samra (SBN 313050)
555 12th Street, Suite 1600
Oakland, CA 94607
Tel.: (415) 445-4003
Fax: (415) 445-4020

[56] *See e.g.*, *supra* note 7; *supra* note 19; *see also* Julia Carrie Wong, *Facebook Acknowledges Concerns over Cambridge Analytica Emerged Earlier than Reported*, The Guardian (Mar. 21, 2019), https://www.theguardian.com/uk-news/2019/mar/21/facebook-knew-of-cambridge-analytica-data-misuse-earlier-than-reported-court-filing (Facebook "heard speculation that Cambridge Analytica was scraping data" months before it had previously represented).

dloeser@kellerrohrback.com
lsarko@kellerrohrback.com
gcappio@kellerrohrback.com
claufenberg@kellerrohrback.com
bgould@kellerrohrback.com

lweaver@bfalaw.com
mweiler@bfalaw.com
adavis@bfalaw.com
ealdridge@bfalaw.com
jsamra@bfalaw.com

Christopher Springer (SBN 291180)
801 Garden Street, Suite 301
Santa Barbara, CA 93101
Tel.: (805) 456-1496
Fax: (805) 456-1497
cspringer@kellerrohrback.com

Plaintiffs' Co-Lead Counsel

ATTESTATION PURSUANT TO CIVIL LOCAL RULE 5-1(i)(3)

I, Lesley E. Weaver, attest that concurrence in the filing of this document has been obtained from the other signatory. I declare under penalty of perjury that the foregoing is true and correct.

Executed this 12th day of April, 2019, at Oakland, California.

/s/ *Lesley E. Weaver*
Lesley E. Weaver

CERTIFICATE OF SERVICE

I, Lesley E. Weaver, hereby certify that on April 12, 2019, I electronically filed the foregoing with the Clerk of the United States District Court for the Northern District of California using the CM/ECF system, which shall send electronic notification to all counsel of record.

/s/ *Lesley E. Weaver*
Lesley E. Weaver

4848-4634-5876, v. 2